KASPERSKY LAB

Kaspersky Internet Security 6.0

BENUTZERHANDBUCH

KASPERSKY INTERNET SECURITY 6.0

Benutzerhandbuch

www.kaspersky.de

Erscheinungsdatum: Januar 2007

Inhalt

KAPITEL 1. BEDROHUNGEN FÜR DIE COMPUTERSICHERHEIT

Aufgrund der rasanten Entwicklung der Informationstechnologien und ihrer Präsenz in allen Lebensbereichen ist die Zahl der Verbrechen, die sich gegen die Informationssicherheit richten, gestiegen.

Auf besonderes Interesse von Cyber-Verbrechern stößt die Tätigkeit staatlicher Einrichtungen und kommerzieller Unternehmen. Ziele sind Diebstahl und Verkauf vertraulicher Informationen, Rufschädigung, Schädigung der Netzwerke und Zugang zu Informationsressourcen einer Organisation. Solche Aktionen verursachen enormen materiellen Schaden und Imageverlust.

Diesem Risiko unterliegen nicht nur Großunternehmen, sondern auch private Nutzer. Mit Hilfe unterschiedlicher Mittel verschaffen sich Verbrecher Zugriff auf persönliche Daten wie Kontonummern, Kreditkartennummern und Kennwörter, machen das System funktionsunfähig oder erhalten vollständigen Zugang auf den Computer. Ein solcher Computer kann als Teil eines so genannten Zombie-Netzes benutzt werden, eines Netzwerks von infizierten Computern, das dazu dient, Angriffe auf Server auszuüben, Spam zu versenden, vertrauliche Informationen zu sammeln, neue Viren und Trojaner zu verbreiten.

Es ist heute allgemein anerkannt, dass Informationen ein wertvolles Gut sind und geschützt werden müssen. Gleichzeitig sollen Informationen aber für einen bestimmten Kreis von Benutzern zugänglich sein (beispielsweise für Mitarbeiter, Kunden und Geschäftspartner). Daraus ergibt sich die Notwendigkeit eines komplexen Systems zur Informationssicherheit. Dieses System muss alle bestehenden Bedrohungsquellen berücksichtigen (menschliche, technische und unvorhersehbare Faktoren) und das gesamte Spektrum von Schutzmaßnahmen verwenden, wozu physikalische, administrative und mit Software und Technik verbundene Schutzwerkzeuge zählen.

1.1. Bedrohungsquellen

Als Quellen für die Bedrohung der Informationssicherheit können eine Einzelperson oder eine Personengruppe, sowie Phänomene, die von menschlicher Tätigkeit unabhängig sind, auftreten. Dadurch lassen sich drei Gruppen von Bedrohungsquellen unterscheiden:

- **Menschlicher Faktor**. Diese Gruppe von Bedrohungen steht mit den Aktionen eines Menschen in Verbindung, der rechtmäßigen oder

unerlaubten Zugriff auf Informationen besitzt. Die Bedrohungen dieser Gruppe können unterteilt werden in:

- *externe*: Dazu zählen Aktionen von Cyber-Verbrechern, Hackern, Internetbetrügern und böswilligen Partnern.
- *interne*: Hierzu gehören die Aktionen von Firmenmitarbeitern und Benutzern von Privat-PCs. Die Handlungen dieser Personen können vorsätzlich oder zufällig sein.

- **Technischer Faktor**. Diese Gruppe von Bedrohungen ist mit technischen Problemen verbunden. Dazu zählen veraltete Geräte sowie mindere Qualität der benutzten Software und Hardware. Diese Faktoren können zur Fehlfunktion von Geräten und zum teilweisen Verlust von Informationen führen.
- **Unvorhersehbarer Faktor**. Diese Gruppe der Bedrohungen umfasst Naturkatastrophen und sonstige Umstände höherer Gewalt, die nicht von menschlicher Tätigkeit abhängig sind.

Alle drei Bedrohungsquellen sollten bei der Organisation eines Schutzsystems berücksichtigt werden. In diesem Handbuch beschreiben wir allerdings nur die Quelle, die direkt mit der Tätigkeit der Firma Kaspersky Lab verbunden ist: die externen Bedrohungen, die mit menschlicher Tätigkeit in Verbindung stehen.

1.2. Ausbreitung der Bedrohungen

Die Entwicklung der modernen Computertechnologien und Kommunikationsmittel verleiht Angreifern die Möglichkeit, unterschiedliche Verbreitungsquellen für Bedrohungen zu benutzen, die im Folgenden genauer beschrieben werden:

Internet

Das Internet zeichnet sich dadurch aus, dass es niemandem gehört und keine territorialen Grenzen besitzt. Das ermöglicht die Entwicklung zahlreicher Web-Ressourcen und den Austausch von Informationen. Jeder Mensch kann Zugriff auf die im Internet gespeicherten Daten erhalten oder seinen eigenen Web-Service anbieten.

Allerdings wird Angreifern eben durch diese Besonderheiten ermöglicht, im Internet Verbrechen zu verüben, die nur schwer erkannt und verfolgt werden können.

Böswillige Personen platzieren Viren und andere Schadprogramme auf Webseiten und tarnen diese als nützliche und kostenlose Software. Außerdem können Skripte, die beim Öffnen von Webseiten automatisch gestartet werden, schädliche Aktionen auf dem Computer ausführen,

unter anderem Modifikation der Systemregistrierung, Diebstahl persönlicher Daten und Installation schädlicher Programme.

Mit Netzwerktechnologien lassen sich Angriffe auf entfernte Privat-PCs und Unternehmensserver verwirklichen. Das Ergebnis solcher Angriffe kann der vollständige Zugriff auf gespeicherte Informationen, sowie der Missbrauch des Rechners als Teil eines Zombie-Netzes sein.

Im Bereich Kreditkartenzahlung, E-Money und Online-Banking (Internet-Shops, -Auktionen, Websites von Banken usw.) hat sich der Internetbetrug zu einem weit verbreiteten Verbrechen entwickelt.

Intranet

Das Intranet ist ein lokales Netzwerk, das den speziellen Erfordernissen der Informationsverwaltung in einem Unternehmen oder in einem privaten Netzwerk entspricht. Ein Intranet stellt einen einheitlichen Raum zum Speichern, Austausch und Zugriff auf Informationen für alle Computer eines Netzwerks dar. Ist ein Computer des Netzwerks infiziert, dann unterliegen die übrigen Computer einem hohen Infektionsrisiko. Um das zu verhindern, müssen nicht nur die Grenzen des Netzwerks geschützt werden, sondern auch jeder einzelne Computer.

E-Mail

Da praktisch auf jedem Computer ein Mailprogramm installiert ist und schädliche Programme auf der Suche nach neuen Opfern den Inhalt elektronischer Adressbücher verwenden, entstehen günstige Bedingungen für die Ausbreitung von Schadprogrammen. Der Benutzer eines infizierten Computers verschickt – ohne selbst Verdacht zu schöpfen – infizierte E-Mails an Adressaten, die ihrerseits neue infizierte Mails weiterschicken usw. Häufig gelangt ein infiziertes Dokument oder eine Datei durch Unachtsamkeit in eine Verteilerliste für kommerzielle Informationen eines Großunternehmens. In diesem Fall sind nicht nur fünf, sondern hunderte oder tausende von Abonnenten solcher Verteiler betroffen, welche die infizierten Dateien wiederum an zehntausende ihrer Abonnenten weiterreichen.

Neben der Gefahr des Eindringens von Schadprogrammen besteht das Problem unerwünschter E-Mails, die Werbung enthalten (Spam). Zwar stellen unerwünschte E-Mails keine direkte Bedrohungsquelle dar, doch erhöhen sie die Belastung von Mailservern, ergeben zusätzlichen Datenverkehr, verstopfen das Benutzerpostfach, führen zu Zeitverlust und verursachen dadurch erhebliche finanzielle Schäden.

Erwähnenswert ist auch, dass Angreifer so genannte Spam-Technologien mit Massencharakter und Methoden des Social Engineering verwenden, um einen Benutzer dazu zu veranlassen, eine E-Mail zu öffnen, über einen Link aus der E-Mail zu einer bestimmten Internetressource zu gehen usw. Deshalb ist die Möglichkeit zur Spam-Filterung auch zum

Kampf gegen neue Arten des Internetbetrugs (wie beispielsweise Phishing) sowie gegen die Verbreitung von Schadprogrammen notwendig.

Wechseldatenträger

Zum Speichern und zur Weitergabe von Informationen sind CDs/DVDs, Disketten und Speichererweiterungskarten (Flash-Cards) weit verbreitet.

Wenn Sie eine Datei, die schädlichen Code enthält, von einem Wechseldatenträger starten, können die auf Ihrem Computer gespeicherten Daten beschädigt werden und ein Virus kann sich auf andere Computerlaufwerke oder Netzwerkcomputer ausbreiten.

1.3. Arten von Bedrohungen

Heutzutage existiert eine große Menge von Bedrohungen, denen Ihr Computer ausgesetzt ist. Dieser Abschnitt bietet eine ausführliche Beschreibung der Bedrohungen, die von Kaspersky Internet Security blockiert werden:

Würmer

Diese Kategorie der schädlichen Programme benutzt in erster Linie die Schwachstellen von Betriebssystemen, um sich auszubreiten. Die Klasse erhielt ihren Namen aufgrund ihrer wurmähnlichen Fähigkeit, von Computer zu Computer "weiter zu kriechen", wobei Netzwerke und E-Mails benutzt werden. Deshalb besitzen Würmer eine relativ hohe Ausbreitungsgeschwindigkeit.

Würmer dringen in einen Computer ein, suchen nach Netzwerkadressen anderer Computer und versenden ihre Kopien an diese Adressen. Neben Netzwerkadressen verwenden Würmer häufig auch Daten aus dem Adressbuch von Mailprogrammen. Vertreter dieser Klasse der schädlichen Programme erstellen teilweise Arbeitsdateien auf Systemlaufwerken, können aber auch ohne jeden Zugriff auf Computerressourcen (mit Ausnahme des Arbeitsspeichers) funktionieren.

Viren

Viren sind Programme, die andere Programme infizieren, indem sie ihnen den eigenen Code hinzufügen, um beim Start infizierter Dateien die Kontrolle zu übernehmen. Diese einfache Definition nennt die *Infektion* als von einem Virus ausgeführte Basisaktion.

Trojaner

Trojaner sind Programme, die auf infizierten Computern unerlaubte Aktionen ausführen, d.h. abhängig von bestimmten Bedingungen die Informationen auf Laufwerken vernichten, das System zum Absturz

bringen, vertrauliche Informationen stehlen usw. Diese Klasse der schädlichen Programme fällt nicht unter die traditionelle Definition eines Virus (d.h. andere Programme oder Daten werden nicht infiziert). Trojanische Programme können nicht selbständig in einen Computer eindringen. Sie werden getarnt als nützliche Software verbreitet. Dabei kann der verursachte Schaden den eines traditionellen Virusangriffs erheblich übersteigen.

In letzter Zeit haben sich Würmer zum häufigsten Typ der Schadprogramme entwickelt, die Computerdaten beschädigen. Danach folgen Viren und Trojaner-Programme. Einige schädliche Programme verbinden die Merkmale von zwei oder gar drei der oben genannten Klassen.

Adware

Adware sind Programme, die ohne Wissen des Benutzers in anderer Software enthalten sind und die Präsentation von Werbung zum Ziel haben. In der Regel ist Adware in Programme integriert, die kostenlos verbreitet werden. Die Werbung erscheint auf der Benutzeroberfläche. Häufig sammeln solche Programme persönliche Benutzerdaten und senden Sie an den Programmautor, ändern bestimmte Browser-Einstellungen (Start- und Such-Seiten, Sicherheitsstufe u.a.), und verursachen vom Benutzer unkontrollierten Datenverkehr. Dadurch kann die Sicherheitsrichtlinie verletzt werden und es können direkte finanzielle Verluste entstehen.

Spyware

Spyware sammelt heimlich Informationen über einen bestimmten Benutzer oder eine Organisation zu sammeln. Die Existenz von Spyware auf einem Computer kann völlig unbemerkt bleiben. In der Regel verfolgt Spyware folgende Ziele:

- Überwachen der Benutzeraktionen auf einem Computer
- Sammeln von Informationen über den Festplatteninhalt. In diesem Fall werden meistens bestimmte Ordner und die Systemregistrierung des Computers gescannt, um eine Liste der installierten Software zu erstellen.
- Sammeln von Informationen über Verbindungsqualität, Verbindungsmethode, Modemgeschwindigkeit usw.

Potentiell gefährliche Anwendungen (Riskware)

Als potentiell gefährlich gelten Anwendungen, die nicht über schädliche Funktionen verfügen, die aber Teil der Entwicklungsumgebung eines Schadprogramms sein können oder von Angreifern als Hilfskomponenten schädlicher Programme verwendet werden können. Zu dieser Kategorie zählen Programme, die Schwachstellen und Fehler enthalten, sowie

Dienstprogramme zur Remote-Administration, Programme zum automatischen Umschalten der Tastaturbelegung, IRC-Clients, FTP-Server und alle Dienstprogramme zum Beenden von Prozessen oder zum Verstecken der Arbeit von Prozessen.

Ein weiterer Typ von Schadprogrammen, die solchen Programmen wie Adware, Spyware und Riskware nahe stehen, sind Programme die in den auf einem Computer installierten Browser integriert werden. Vielleicht sind Sie schon auf solche Programme gestoßen, wenn beim Aufruf einer Webseiten-Adresse eine ganz andere Seite geöffnet wurde.

Scherzprogramme (Jokes)

Jokes sind Programme, die dem Computer keinen direkten Schaden zufügen, sondern Meldungen darüber anzeigen, dass bereits Schaden verursacht wurde oder unter bestimmten Bedingungen Schaden angerichtet wird. Solche Programme warnen den Benutzer häufig vor fiktiven Gefahren. So kann beispielsweise eine Meldung angezeigt werden, die über das Formatieren der Festplatte informiert (obwohl dies nicht der Wirklichkeit entspricht) oder einen Virusfund in Dateien meldet, die aber tatsächlich virusfrei sind.

Rootkits

Rootkits sind Dienstprogramme, die der Tarnung von schädlichen Prozessen dienen. Sie maskieren schädliche Programme, um zu vermeiden, dass diese von Antiviren-Programmen gefunden werden. Rootkits sind außerdem fähig, das Betriebssystem des Computers zu modifizieren und dessen Grundfunktionen zu ersetzen, wodurch sie die eigene Existenz und Aktionen, die ein Angreifer auf dem infizierten Computer vornimmt, verbergen.

Andere gefährliche Programme

Dazu zählen Programme, die der Organisation von DoS-Angriffen auf entfernte Server, dem Eindringen in andere Computer und dem Erstellen schädlicher Software dienen. Zu diesen Programmen gehören Hackerdienstprogramme (Hack-Tools), Virenkonstrukteure, Schwachstellen-Scanner, Programme zum Kennwort-Diebstahl sowie sonstige Programme zum Einbruch in Netzwerkressourcen oder zum Eindringen in ein angegriffenes System.

Hackerangriffe

Hackerangriffe sind Aktionen böswilliger Personen oder schädlicher Programme, die sich auf die Übernahme von Daten eines entfernten Computers, auf die Beschädigung der Funktionstüchtigkeit eines Systems oder auf die vollständige Kontrolle über Computerressourcen beziehen. Eine ausführliche Beschreibung der Angriffe, die von Kaspersky Internet

Security blockiert werden, befindet sich im Abschnitt Liste der erkennbaren Netzwerkangriffe.

Bestimmte Arten des Internetbetrugs

Phishing ist eine Art des Internetbetrugs, die im Versenden von E-Mails besteht, um vertrauliche finanzielle Informationen zu stehlen. Phishing-Mails sind so gestaltet, dass sie möglichst große Ähnlichkeit mit Informationsbriefen von Banken oder bekannten Firmen besitzen. Die Nachrichten verweisen auf eine gefälschte Seite, die vom Angreifer speziell vorbereitet wurde und eine Kopie der Seite jener Organisation darstellt, von der die Mail scheinbar stammt. Auf dieser Seite wird der Benutzer beispielsweise aufgefordert, seine Kreditkartennummer oder andere vertrauliche Informationen anzugeben.

Einwahl auf kostenpflichtige Internetseiten – Diese Art des Internetbetrugs besteht in der unerlaubten Verwendung kostenpflichtiger Internetressourcen (meist Webseiten mit pornografischem Inhalt). Die von Angreifern installierten Programme (Dialer) initiieren eine Modemverbindung Ihres Computers mit einer kostenpflichtigen Nummer. Solche Nummern werden meistens nach überhöhten Tarifen abgerechnet, was für den Benutzer eine sehr hohe Telefonrechnung zur Folge hat.

Aufdringliche Werbung

Als aufdringliche Werbung gelten Popup-Fenster und Werbebanner, die sich auf Webseiten öffnen. In der Regel sind die darin enthaltenen Informationen nicht nützlich, sondern lenken den Benutzer von seiner eigentlichen Arbeit ab und erhöhen den Datenverkehr.

Spam

Spam ist der anonyme Massenversand von unerwünschten E-Mails. Spam kann politischen und agitatorischen Charakter besitzen oder karitative Appelle enthalten. Eine bestimmte Spam-Kategorie umfasst Briefe mit einer Aufforderung, an der "Geldwäsche" hoher Summen oder an einer Finanzpyramide teilzunehmen, sowie Briefe, die den Diebstahl von Kennwörtern und Kreditkartennummern verfolgen, Kettenbriefe (z.B. Glücksbriefe) usw. Spam erhöht die Belastung von Mailservern und das Risiko des Verlusts wichtiger Informationen erheblich.

Das Erkennen und Blockieren dieser Arten von Bedrohungen wird von Kaspersky Internet Security über zwei Methoden ausgeführt:

- *reaktiv* – Diese Methode beruht auf der Suche von schädlichen Objekten mit Hilfe der laufend aktualisierten Datenbank der Bedrohungssignaturen.
- *proaktiv* – Im Unterschied zum reaktiven Schutz basiert diese Methode nicht auf der Code-Analyse eines Objekts, sondern auf der Analyse

seines Verhaltens im System. Diese Methode ermöglicht das Erkennen neuer Gefahren, über die noch keine Informationen in den Datenbanken vorhanden sind.

Die Verwendung beider Methoden in Kaspersky Internet Security gewährleistet den kompletten Schutz Ihres Computers vor bekannten und neuen Bedrohungen.

1.4. Kennzeichen einer Infektion

Es existiert eine Reihe von Kennzeichen, die auf eine Computerinfektion hinweisen. Wenn Sie bemerken, dass sich der Computer beispielsweise auf folgende Weise "seltsam" verhält, dann ist er mit hoher Wahrscheinlichkeit von einem Virus infiziert:

- Es werden unvorhergesehene Meldungen oder Bilder auf dem Bildschirm angezeigt oder unvorhergesehene Audiosignale wiedergegeben.
- Die Schublade des CD/DVD-ROM-Laufwerks öffnet und schließt sich ohne erkennbaren Grund.
- Bestimmte Programme auf dem Computer werden willkürlich gestartet, ohne dass dies von Ihnen initiiert wurde.
- Auf dem Bildschirm werden Meldungen angezeigt, die sich auf den Versuch bestimmter Programme Ihres Computers beziehen, eine Verbindung mit dem Internet herzustellen, obwohl Sie dies nicht initiiert haben.

Außerdem gibt es einige charakteristische Merkmale für eine Virusinfektion durch E-Mails:

- Freunde oder Bekannte teilen Ihnen mit, dass sie Nachrichten von Ihnen erhalten haben, die Sie aber nicht abgeschickt haben.
- In Ihrer Mailbox befindet sich eine große Anzahl von Nachrichten ohne Antwortadresse und Betreff.

Es ist anzumerken, dass diese Merkmale nicht immer durch die Existenz von Viren hervorgerufen werden. Manchmal können sie auf andere Ursachen zurückgehen. So können beispielsweise infizierte Nachrichten zwar Ihre Adresse als Antwortadresse enthalten, aber trotzdem von einem anderen Computer aus abgeschickt worden sein.

Außerdem existieren indirekte Hinweise auf eine Infektion Ihres Computers:

- häufiges Abstürzen und Funktionsstörungen des Computers.
- verlangsamter Start von Programmen.

- das Laden des Betriebssystems ist nicht möglich.
- Verschwinden von Dateien und Ordnern oder Veränderungen ihres Inhalts.
- häufiger Zugriff auf die Festplatte (häufiges Blinken der Festplatten-LED am PC-Gehäuse).
- Der Webbrowser (z.B. Microsoft Internet Explorer) "bleibt hängen" oder verhält sich unerwartet (z.B. das Programmfenster lässt sich nicht schließen).

In 90 % der Fälle werden indirekte Symptome durch Hardware- oder Softwarestörungen verursacht. Trotz der geringen Wahrscheinlichkeit, dass solche Symptome auf eine Infektion zurückgehen, wird bei ihrem Auftreten empfohlen, die vollständige Untersuchung Ihres Computers (s. 5.2 auf S. 66) mit den von Kaspersky Lab empfohlenen Einstellungen vorzunehmen.

1.5. Was tun, wenn Kennzeichen einer Infektion auftreten?

Wenn Sie bemerken, dass sich Ihr Computer "verdächtig verhält",

1. Keine Panik! Diese goldene Regel kann Sie vor dem Verlust wichtiger Daten und unnötigem Stress bewahren.
2. Trennen Sie den Computer vom Internet und vom lokalen Netzwerk, wenn er damit verbunden ist.
3. Wenn das Symptom darin besteht, dass der Systemstart von der Festplatte des Computers nicht möglich ist (der Computer gibt einen Fehler aus, wenn Sie ihn einschalten), versuchen Sie, das System im abgesicherten Modus oder von der Microsoft Windows-Rettungsdiskette zu starten, die Sie bei der Installation des Betriebssystems auf dem Computer erstellt haben.
4. Bevor Sie irgendwelche Aktionen ausführen, speichern Sie Ihre Daten auf einem externen Datenträger (Diskette, CD/DVD, Flash-Card usw.).
5. Installieren Sie Kaspersky Internet Security, falls er noch nicht installiert wurde.
6. Aktualisieren Sie die Bedrohungssignaturen und die Anwendungsmodule (s. 5.6 auf S. 70). Verwenden Sie für den Download aus dem Internet möglichst nicht Ihren eigenen Computer, sondern einen virusfreien Computer (Computer eines Freundes, im Internet-Café, bei der Arbeit). Die Verwendung eines anderen Computers ist von Vorteil, da bei einer Internetverbindung des

infizierten Computers die Möglichkeit besteht, dass der Virus wichtige Informationen an die Angreifer sendet oder sich an die Adressen Ihres Adressbuchs verschickt. Gerade deshalb sollte bei einem Infektionsverdacht die Verbindung mit dem Internet sofort getrennt werden.

7. Stellen Sie die von Kaspersky Lab empfohlene Schutzstufe ein.
8. Starten Sie die vollständige Untersuchung des Computers (s. 5.2 auf S. 66).

1.6. Sicherheitsregeln

Selbst die zuverlässigsten und vernünftigsten Maßnahmen können keinen hundertprozentigen Schutz vor Computerviren und Trojaner bieten. Allerdings lässt sich das Risiko einer Virusinfektion und möglicher Verluste minimieren, indem Sie folgende Regeln beachten.

Eine der wichtigsten Methoden im Kampf gegen Viren ist, wie auch in der Medizin, die rechtzeitige *Prophylaxe*. Die Computerprophylaxe umfasst wenige Regeln, welche die Wahrscheinlichkeit einer Virusinfektion und des Datenverlusts erheblich verringern.

Im Folgenden finden Sie die wichtigsten Sicherheitsregeln zur Vermeidung von Virusinfektionen.

Regel 1: *Schützen Sie Ihren Computer mit Hilfe eines Antiviren-Programms und einer Firewall*:

- Installieren Sie umgehend Kaspersky Internet Security.
- Aktualisieren Sie regelmäßig die Bedrohungssignaturen, die zum Umfang des Programms gehören. Das Update kann beim Eintreten einer Virusepidemie mehrmals täglich vorgenommen werden. In solchen Fällen werden die Datenbanken der bekannten Bedrohungen auf den Updateservern von Kaspersky Lab unverzüglich aktualisiert.
- Legen Sie die von Kaspersky Lab empfohlenen Einstellungen für den Schutz Ihres Computers fest. Der Echtzeitschutz wird sofort nach dem Hochfahren des Computers wirksam und erschwert Viren das Eindringen in den Computer.
- Legen Sie die von Kaspersky Lab empfohlenen Einstellungen für die vollständige Untersuchung des Computers fest und planen Sie deren Ausführung mindestens einmal pro Woche. Wenn Sie die Komponente Anti-Hacker nicht installiert haben, wird deren Installation empfohlen, um den Computer bei der Arbeit im Internet zu schützen.

Regel 2: *Verhalten Sie sich beim Speichern neuer Daten auf dem Computer vorsichtig*:

- Untersuchen Sie alle Wechseldatenträger (s. 5.6 Auf S. 70) (Disketten, CDs/DVDs, Flash-Cards usw.) vor deren Verwendung auf das Vorhandensein von Viren.
- Gehen Sie vorsichtig mit E-Mail-Nachrichten um. Starten Sie nie Dateien, die Sie per E-Mail erhalten haben, wenn Sie nicht sicher sind, dass diese wirklich für Sie bestimmt sind, selbst wenn diese von einem Bekannten abgeschickt wurden.
- Gehen Sie vorsichtig mit allen Daten um, die Sie aus dem Internet empfangen haben. Wenn Ihnen von einer Webseite angeboten wird, ein neues Programm zu installieren, vergewissern Sie sich über das Vorhandensein eines Sicherheitszertifikats.
- Wenn Sie eine ausführbare Datei aus dem Internet oder über ein lokales Netzwerk herunterladen, dann untersuchen Sie diese unbedingt mit Kaspersky Internet Security.
- Verhalten Sie sich vorsichtig bei der Auswahl der von Ihnen besuchten Internetressourcen. Bestimmte Seiten sind von gefährlichen Skriptviren oder Internetwürmern infiziert.

Regel 3: *Verfolgen Sie aufmerksam die Informationen von Kaspersky Lab*.

In den meisten Fällen informiert Kaspersky Lab über den Ausbruch einer neuen Epidemie lange bevor diese ihren Höhepunkt erreicht. Die Wahrscheinlichkeit einer Infektion ist in diesem Fall noch gering und durch den Download der aktualisierten Bedrohungssignaturen können Sie sich rechtzeitig vor einem neuen Virus schützen.

Regel 4: *Verhalten Sie sich misstrauisch gegenüber falschen Viruswarnungen,* Scherzprogrammen und E-Mails, die vorgeben vor Infektionen zu warnen.

Regel 5: *Verwenden Sie den Dienst Windows Update und* installieren Sie regelmäßig die Updates für das Betriebssystem Microsoft Windows.

Regel 6: *Kaufen Sie Ihre Software nur bei offiziellen Händlern*.

Regel 7: *Beschränken Sie den Kreis der Leute, die zur Arbeit auf Ihrem Computer berechtigt sind*.

Regel 8: *Verringern Sie das Risiko unangenehmer Folgen einer möglichen Infektion*:

- Fertigen Sie rechtzeitig Sicherungskopien Ihrer Daten an. Wenn Sicherungskopien vorhanden sind, kann das System bei Datenverlust schnell wiederhergestellt werden. Distributions-CDs, Disketten, Flash-Cards und andere Datenträger mit Software und wertvollen Informationen sollten an einem sicheren Ort aufbewahrt werden.

- Erstellen Sie unbedingt eine Notfall-CD (s. 5.4 Auf S. 68), von der Sie Ihren Computer bei Bedarf unter Verwendung eines "sauberen" Betriebssystems starten können.

Regel 9: *Überprüfen Sie regelmäßig die Liste der auf Ihrem Computer installierten Programme.* Dazu können Sie den Punkt **Programme ändern oder entfernen** in der **Systemsteuerung** verwenden oder einfach den Inhalt des Ordners **Programme** und des Autostart-Ordners überprüfen. Dadurch können Sie Software finden, die ohne Ihr Wissen auf dem Computer installiert wurde, während Sie beispielsweise das Internet benutzt oder ein bestimmtes Programm installiert haben. Möglicherweise befinden sich potentiell gefährliche Programme darunter.

KAPITEL 2. KASPERSKY INTERNET SECURITY 6.0

Kaspersky Internet Security 6.0 ist die neue Generation des Informationsschutzes.

Der Hauptunterschied zwischen Kaspersky Internet Security 6.0 und anderen Produkten, einschließlich anderer Kaspersky-Lab-Produkte, besteht in der komplexen Methode zum Schutz der Daten auf dem Computer.

2.1. Was ist neu in Kaspersky Internet Security 6.0

Kaspersky Internet Security 6.0 bietet eine prinzipiell neue Methode zum Datenschutz. Das wichtigste Merkmal des Programms besteht darin, dass verschiedene Funktionen in einer komplexen Lösung vereinigt und bedeutend optimiert wurden. Das Programm bietet nicht nur einen Virenschutz, sondern auch Spam-Schutz und Schutz vor Hackerangriffen. Neue Module ermöglichen den Schutz vor unbekannten Bedrohungen, vor Phishing und Programmen, die schädliche Aktivitäten tarnen.

Künftig ist es überflüssig, mehrere Produkte auf dem Computer zu installieren, um einen vollständigen Schutz zu garantieren. Die Installation von Kaspersky Internet Security 6.0 ist ausreichend.

Der komplexe Schutz wird auf allen Kanälen gewährleistet, auf denen Daten eingehen und übertragen werden. Die flexible Konfiguration aller Programmkomponenten erlaubt die Anpassung von Kaspersky Internet Security 6.0 an Ihre Anforderungen. Außerdem können alle Schutzkomponenten unter einer Oberfläche konfiguriert werden.

Im Folgenden werden die neuen Optionen von Kaspersky Internet Security 6.0 ausführlich beschrieben.

Neuerungen im Schutz

- Kaspersky Internet Security schützt nicht nur vor bekannten schädlichen Programmen, sondern auch vor solchen, die noch unbekannt sind. Die Komponente Proaktiver Schutz (s. Kapitel 10 auf S. 133) stellt einen der wichtigsten Vorzüge des Programms dar. Ihre Arbeit beruht auf der Analyse des Verhaltens der auf Ihrem Computer installierten Anwendungen, der Kontrolle von Veränderungen in der

Systemregistrierung, der Überwachung der Makroausführung und dem Kampf gegen versteckte Bedrohungen. Bei der Arbeit der Komponente wird eine heuristische Analyse verwendet, die es erlaubt, unterschiedliche Arten von Schadprogrammen zu erkennen. Hierbei wird ein Bericht geführt, auf dessen Basis Aktionen, die von Schadprogrammen ausgeführt wurden, rückgängig gemacht werden können und der Systemszustand vor der schädlichen Veränderung wiederhergestellt werden kann.

- Der Schutz vor Tarnprogrammen und vor Programmen zur automatischen Einwahl auf kostenpflichtige Webseiten, das Blockieren von Bannern, Popup-Fenstern und schädlichen Skripts, die von Internetseiten geladen werden, sowie das Erkennen von Phishing-Seiten werden gewährleistet.

- Die Technologie für den Schutz der Dateien auf dem Benutzercomputer wurde verbessert: Sie können nun die Belastung des Zentralprozessors und der Laufwerkssubsysteme senken und die Untersuchungsgeschwindigkeit erhöhen. Dies wird durch die Verwendung der Technologien iChecker™ und iSwift™ erreicht. Dieser Modus schließt die wiederholte Prüfung von Dateien aus.

- Der Prozess zur Virensuche wird nun Ihrer Arbeit auf dem Computer untergeordnet. Eine Untersuchung kann relativ viel Zeit und Systemressourcen beanspruchen, trotzdem kann der Benutzer gleichzeitig seine Arbeit ausführen. Wenn das Ausführen einer bestimmten Operation Systemressourcen erfordert, wird die Virensuche bis zum Abschluss dieser Operation angehalten. Danach wird die Untersuchung an der Stelle fortgesetzt, an dem sie angehalten wurde.

- Der Untersuchung kritischer Computerbereiche, deren Infektion ernste Folgen haben kann, ist eine separate Aufgabe zugeordnet. Sie können diese Aufgabe so konfigurieren, dass sie jedes Mal beim Systemstart automatisch gestartet wird.

- Der Schutz von E-Mails vor schädlichen Programmen und Spam wurde wesentlich verbessert. Das Programm untersucht den E-Mailstrom folgender Protokolle auf Viren:

    - IMAP, SMTP, POP3, unabhängig vom verwendeten Mailprogramm.

    - NNTP (nur Virenuntersuchung), unabhängig vom verwendeten Mailprogramm.

    - Unabhängig vom Protokolltyp (einschließlich MAPI, HTTP) im Rahmen der Arbeit der in die Mailprogramme Microsoft Office Outlook und The Bat! integrierten PlugIns.

- In bekannte Mailprogramme wie Microsoft Office Outlook, Microsoft Outlook Express und The Bat! wird ein spezielles Erweiterungsmodul

(PlugIn) integriert, das die Konfiguration des E-Mail-Schutzes vor Viren und Spam direkt im Mailprogramm erlaubt.

- Das Training von Anti-Spam erfolgt mit den Briefen Ihrer Mailbox. Dabei werden alle Besonderheiten Ihrer Arbeit mit E-Mails berücksichtigt und die flexible Konfiguration des Spam-Schutzes erlaubt. Das Training basiert auf dem iBayes-Algorithmus. Zusätzlich können Sie schwarze und weiße Listen mit Adressaten und Schlüsselphrasen anlegen, auf Grund derer die Spam-Erkennung erfolgt.

  Bei der Arbeit von Anti-Spam wird eine Phishing-Datenbank verwendet. Sie erlaubt es, Briefe auszufiltern, deren Ziel im Diebstahl vertraulicher Informationen besteht.

- Das Programm gewährleistet die Filterung des eingehenden und ausgehenden Datenverkehrs, überwacht und verhindert Bedrohungen durch verbreitete Netzwerkangriffe und erlaubt es, den "Tarnmodus" für die Arbeit im Netzwerk zu verwenden.

- Bei der Arbeit in einem Netzwerk, können Sie bestimmen, welches Netzwerk hundertprozentig vertrauenswürdig ist und welches mit höchster Vorsicht überwacht werden soll.

- Die Funktion zur Benachrichtigung des Benutzers (s. Pkt. 17.11.1 auf S. 299) über bestimmte Ereignisse während der Programmarbeit wurde erweitert. Für jeden Ereignistyp kann eine Benachrichtigungsmethode festgelegt werden: E-Mail-Nachricht, Audiosignal, Popup-Meldung, Eintrag im Ereignisbericht.

- Die Untersuchung des über eine durch SSL-Protokoll geschützte Verbindung übertragenen Datenstroms wurde realisiert.

- Eine Technologie zum Selbstschutz der Anwendung, zum Schutz vor unerlaubter Fernsteuerung des Diensts Kaspersky Internet Security sowie zum Kennwortschutz für den Zugriff auf die Anwendungseinstellungen wurde hinzugefügt. Dadurch kann verhindert werden, dass schädliche Programme, Angreifer oder unqualifizierte Benutzer den Schutz ausschalten.

- Eine Option zum Erstellen einer Notfall-CD für die Systemwiederherstellung wurde hinzugefügt. Mit Hilfe dieser CD lässt sich nach einem Virenangriff das Betriebssystem laden und der Computer kann auf die Existenz schädlicher Objekte untersucht werden.

Neuerungen auf der Programmoberfläche

- Auf der neuen Oberfläche von Kaspersky Internet Security ist der einfache und komfortable Zugriff auf alle Programmfunktionen realisiert. Außerdem lässt sich das Programmdesign durch die Verwendung eigener grafischer Elemente und Farbschemen anpassen.

- Bei der Arbeit mit dem Programm erhalten Sie vollständige Informationen: Kaspersky Internet Security zeigt Meldungen über den Schutzstatus an, begleitet seine Arbeit durch Kommentare sowie Tipps und besitzt ein ausführliches Hilfesystem.

Neuerungen beim Programmupdate

- In dieser Anwendungsversion wurde eine optimierte Updateprozedur realisiert: Kaspersky Internet Security kontrolliert nun automatisch, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Wenn neue Updates gefunden werden, lädt die Anwendung sie herunter und installiert sie auf dem Computer.
- Nur fehlende Updates werden heruntergeladen. Dadurch lässt sich das Volumen des beim Update notwendigen Netzwerkverkehrs bis um das Zehnfache verringern.
- Die Aktualisierung erfolgt von der effektivsten Updatequelle.
- Es besteht die Möglichkeit, keinen Proxyserver zu verwenden, wenn das Programmupdate über eine lokale Quelle erfolgt. Dadurch wird das Volumen des Netzwerkverkehrs über den Proxyserver erheblich vermindert.
- Eine Option zum Rückgängigmachen von Updates wurde realisiert. Dadurch wird beispielsweise bei einer Beschädigung von Dateien oder bei einem Kopierfehler erlaubt, zur vorhergehenden Version der Bedrohungssignaturen zurückzukehren.
- Eine Option zum Verwenden eines Diensts für die Update-Verteilung in einen lokalen Ordner wurde hinzugefügt. Wird anderen Netzwerkcomputern Zugriff auf den Ordner gewährt, dann lässt sich Internet-Datenverkehr einsparen.

2.2. Die Schutzprinzipien von Kaspersky Internet Security

Der Schutz von Kaspersky Internet Security wird von den Bedrohungsquellen ausgehend aufgebaut. Für jede Quelle ist eine separate Programmkomponente vorgesehen, die ihre Kontrolle und notwendige Maßnahmen zur Verhinderung schädlicher Einwirkungen dieser Quelle auf die Benutzerdaten gewährleistet. Diese Konzeption des Schutzsystems erlaubt es, die Anwendung flexibel einzusetzen und den Erfordernissen eines konkreten Benutzers oder Unternehmens anzupassen.

Kaspersky Internet Security umfasst:

- Schutzkomponenten (s. Pkt. 2.2.1 auf S. 27), die den Schutz Ihres Computers auf allen Kanälen gewährleisten, auf denen Daten empfangen und übertragen werden.
- Aufgaben zur Virensuche (s. Pkt. 2.2.2 auf S. 29), mit deren Hilfe die Untersuchung des Computers und einzelner Dateien, Ordner, Laufwerke oder Bereiche ausgeführt wird.
- Servicefunktionen (s. Pkt. 2.2.3 auf S. 30), die Informationen über die Arbeit mit dem Programm bieten und es erlauben, die Programmfunktionalität zu erweitern.

2.2.1. Schutzkomponenten

Der Echtzeitschutz Ihres Computers wird durch folgende Schutzkomponenten gewährleistet:

Datei-Anti-Virus

Das Dateisystem kann Viren und andere gefährliche Programme enthalten. Nachdem Schadprogramme über einen Wechseldatenträger oder das Internet eingedrungen sind, können sie sich jahrelang in Ihrem Dateisystem befinden, ohne dass ihre Existenz bemerkt wird. Sobald eine infizierte Datei aber geöffnet wird, kann der Virus aktiv werden.

Datei-Anti-Virus ist eine Komponente, die das Dateisystem des Computers kontrolliert. Sie untersucht auf Ihrem Computer und auf allen angeschlossenen Laufwerken alle Dateien, die GEÖFFNET, GESTARTET und GESPEICHERT werden. Jeder Zugriff auf eine Datei wird von der Anwendung abgefangen und die Datei wird auf die Existenz bekannter Viren untersucht. Die weitere Arbeit mit der Datei ist nur dann möglich, wenn die Datei virusfrei ist oder erfolgreich von Anti-Virus desinfiziert wurde. Wenn die Desinfektion der Datei aus bestimmten Gründen nicht möglich ist, wird sie gelöscht, wobei eine Kopie der Datei im Backup (s. Pkt. 17.2 auf S. 262) abgelegt oder in der Quarantäne (s. Pkt. 17.1 auf S. 258) gespeichert wird.

Mail-Anti-Virus

Die E-Mail-Korrespondenz wird von Angreifern häufig zur Verbreitung schädlicher Programme verwendet. Sie ist eines der wichtigsten Medien zur Verbreitung von Würmern. Deshalb ist es äußerst wichtig, alle E-Mail-Nachrichten zu kontrollieren.

Mail-Anti-Virus ist eine Komponente zur Untersuchung aller ein- und ausgehenden E-Mail-Nachrichten Ihres Computers. Sie analysiert E-Mails auf Schadprogramme. Eine E-Mail wird nur dann zugestellt, wenn sie keine gefährlichen Objekte enthält.

Web-Anti-Virus

Wenn Sie im Internet bestimmte Webseiten öffnen, riskieren Sie, dass Ihr Computer durch Viren infiziert wird, die mit Hilfe von auf Webseiten enthaltenen Skripts auf dem Computer installiert werden. Außerdem kann ein gefährliches Objekt auf Ihren Computer geladen werden.

Web-Anti-Virus wurde speziell zur Verhinderung solcher Situationen entwickelt. Skripte, die sich auf Webseiten befinden und gefährlich sind, werden von dieser Komponente abgefangen und ihre Ausführung wird gesperrt. Auch der HTTP-Verkehr unterliegt einer strengen Kontrolle.

Proaktiver Schutz

Die Zahl der schädlichen Programme nimmt jeden Tag zu. Malware wird komplizierter, mehrere Arten werden miteinander kombiniert und die Ausbreitungsmethoden immer besser getarnt.

Um ein neues Schadprogramm zu erkennen, bevor es Schaden anrichten kann, hat Kaspersky Lab eine spezielle Komponente entwickelt: Den *Proaktiven Schutz*. Er basiert auf der Kontrolle und Analyse des Verhaltens aller Programme, die auf Ihrem Computer installiert sind. Aufgrund der auszuführenden Aktionen entscheidet Kaspersky Internet Security, ob ein Programm potentiell gefährlich ist oder nicht. So ist Ihr Computer nicht nur vor bekannten Viren, sondern auch vor neuen, bisher unbekannten Viren geschützt.

Anti-Spy

In letzter Zeit nimmt die Ausbreitung von Programmen, die Werbematerialien (Banner, Popup-Fenster) anzeigen, Programmen zur unerlaubten Einwahl auf kostenpflichtige Internetressourcen, Mitteln zur entfernten Verwaltung und Überwachung, Scherzprogrammen, u.a. stark zu.

Anti-Spy überwacht diese Aktionen auf Ihrem Computer und blockiert ihre Ausführung. Die Komponente blockiert beispielsweise die Anzeige von Bannern und Popup-Fenstern, die den Benutzer bei der Arbeit stören, blockiert Programme, die ohne Erlaubnis des Benutzers versuchen, Telefonnummern zu wählen, und analysiert Webseiten auf Phishing-Betrugsversuche.

Anti-Hacker

Hacker verwenden unterschiedlichste Schlupflöcher wie offene Ports, Datenübertragung zwischen zwei Computern usw., um in Ihren Computer einzudringen.

Anti-Hacker ist eine Komponente, die zum Schutz Ihres Computers im Internet und in anderen Netzwerken dient. Sie kontrolliert ausgehende und eingehende Verbindungen und überwacht Ports und Datenpakete.

Anti-Spam

Obwohl Spam keine direkte Bedrohungsquelle darstellt, steigert unerwünschte Korrespondenz die Belastung von Mailservern, verschmutzt das Benutzerpostfach und führt zu Zeitverlust und bedeutenden finanziellen Schäden.

Die Komponente *Anti-Spam* wird in das auf Ihrem Computer installierte Mailprogramm integriert und kontrolliert alle eingehenden E-Mail-Nachrichten auf Spam. Alle E-Mails, die Spam enthalten, werden durch eine spezielle Kopfzeile markiert. Außerdem kann in Anti-Spam die Spam-Bearbeitung (automatisches Löschen, Verschieben in einen speziellen Ordner, u.a.) eingestellt werden.

2.2.2. Aufgaben zur Virensuche

Neben dem Echtzeitschutz aller Quellen, aus denen Schadprogramme eindringen können, ist es sehr wichtig, regelmäßig die vollständige Virenuntersuchung Ihres Computers durchzuführen. Das ist erforderlich, um zu verhindern, dass sich schädliche Programme ausbreiten, die nicht von den Schutzkomponenten erkannt wurden, weil beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Zur Virensuche verfügt Kaspersky Internet Security über drei Aufgaben:

Kritische Bereiche

Virenuntersuchung aller kritischen Computerbereiche. Dazu gehören: Systemspeicher, Objekte, die beim Systemstart ausgeführt werden, Laufwerksbootsektoren und *Windows*-Systemverzeichnisse. Das Ziel dieser Aufgabe besteht im schnellen Erkennen aktiver Viren im System, ohne den Computer vollständig zu untersuchen.

Arbeitsplatz

Virensuche auf Ihrem Computer mit sorgfältiger Untersuchung aller angeschlossenen Laufwerke, des Arbeitsspeichers und der Dateien.

Autostart-Objekte

Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden, sowie des Arbeitsspeichers und der Laufwerks-bootsektoren.

Außerdem besteht die Möglichkeit, andere Aufgaben zur Virensuche zu erstellen und einen Startzeitplan dafür anzulegen. Es kann beispielsweise eine Aufgabe zur wöchentlichen Untersuchung von Maildatenbanken oder eine Aufgabe zur Virensuche im Ordner **Eigene Dateien** erstellt werden.

2.2.3. Servicefunktionen des Programms

Kaspersky Internet Security verfügt über eine Reihe von Servicefunktionen. Sie dienen dazu, den aktuellen Zustand des Programms aufrechtzuerhalten, die Optionen des Programms zu erweitern und bei der Arbeit Hilfe zu leisten.

Update

Um stets bereit zu sein, einen beliebigen Hackerangriff abzuwehren und Viren oder andere gefährliche Programme unschädlich zu machen, muss der aktuelle Zustand von Kaspersky Internet Security aufrechterhalten werden. Dazu ist die Komponente *Update* vorgesehen. Sie dient zur Aktualisierung der Bedrohungssignaturen und Programm-Module von Kaspersky Internet Security, die bei der Arbeit des Programms verwendet werden.

Der Dienst zum Verteilen von Updates erlaubt es, die von den Kaspersky-Lab-Servern heruntergeladenen Updates für die Datenbanken der Bedrohungssignaturen, Netzwerkangriffe und Netzwerktreiber sowie für die Programm-Module in einem lokalen Ordner zu speichern, um dann anderen Netzwerkcomputern den Zugriff auf diesen Ordner zu gewähren und dadurch Internet-Datenverkehr einzusparen.

Datenverwaltung

Während der Arbeit des Programms wird für jede Schutzkomponente, für jede Aufgabe zur Virensuche und für Programmupdates ein Bericht erstellt. Er enthält Informationen über die ausgeführten Operationen und Arbeitsergebnisse. Durch die Verwendung der Funktion *Berichte* können Sie sich jederzeit Details über die Arbeit einer beliebigen Komponente von Kaspersky Internet Security informieren. Beim Auftreten von Problemen können Berichte an Kaspersky Lab gesendet werden, um die Situation durch unsere Spezialisten zu analysieren und Ihnen so schnell wie möglich zu helfen.

Alle Objekte, die hinsichtlich der Sicherheit verdächtig sind, werden von Kaspersky Internet Security in den speziell dafür vorgesehen *Quarantäne-Speicher* verschoben. Sie werden in verschlüsselter Form gespeichert, um eine Infektion des Computers zu vermeiden. Sie können diese Objekte auf Viren untersuchen, am ursprünglichen Ort wiederherstellen, löschen und der Quarantäne selbständig Objekte hinzufügen. Alle Objekte, die sich aufgrund von Ergebnissen der Virenuntersuchung als virusfrei erweisen, werden automatisch am ursprünglichen Ort wiederhergestellt.

Im *Backup* werden Kopien der vom Programm desinfizierten und gelöschten Objekte gespeichert. Diese Kopien werden erstellt, um bei Bedarf Objekte oder ein Bild der Infektion wiederherzustellen. Die

Sicherheitskopien werden in verschlüsselter Form gespeichert, um eine Infektion des Computers zu vermeiden.

Sie können ein Objekt aus dem Backup am ursprünglichen Ort wiederherstellen oder die Kopie löschen.

Notfall-CD

Kaspersky Internet Security enthält einen speziellen Dienst, der es erlaubt, eine Notfall-CD zur Systemwiederherstellung zu erstellen.

Das Erstellen einer solchen CD kann nützlich sein, wenn aufgrund eines Virenangriffs Systemdateien beschädigt wurden und das Betriebssystem nicht mehr geladen werden kann. In diesem Fall können Sie unter Verwendung der Notfall-CD den Computer starten und das System in dem Zustand wiederherstellen, der vor der schädlichen Einwirkung herrschte.

Support

Alle registrierten Benutzer von Kaspersky Internet Security können den technischen Support-Service in Anspruch nehmen. Verwenden Sie die Funktion *Support*, um zu erfahren, wo Sie technische Unterstützung erhalten können.

Mit Hilfe der entsprechenden Links gelangen Sie zum Forum für die Benutzer von Kaspersky-Lab-Produkten und können eine Liste mit häufigen Fragen (FAQ) konsultieren, die Ihnen bei der Lösung eines Problems behilflich sein können. Außerdem können Sie eine Nachricht über einen Fehler oder ein Feedback über die Arbeit der Anwendung an den technischen Kundendienst schicken. Dazu dient ein spezielles Formular auf der Webseite.

Daneben steht Ihnen der Online-Service des technischen Kundendiensts zur Verfügung. Natürlich sind unsere Mitarbeiter jederzeit bereit, Ihnen telefonisch bei der Arbeit mit Kaspersky Internet Security zu helfen.

2.3. Hardware- und Softwarevoraussetzungen

Um die normale Funktionsfähigkeit von Kaspersky Internet Security 6.0 zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen.

Allgemeine Voraussetzungen:

- 50 MB freier Speicher auf der Festplatte

- CD-ROM-Laufwerk (zur Installation von Kaspersky Internet Security 6.0 von CD-ROM).
- Microsoft Internet Explorer Version 5.5 oder höher (für das Update der Bedrohungssignaturen und Programm-Module über das Internet)
- Microsoft Windows Installer 2.0.

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Prozessor Intel Pentium 300 MHz oder höher (oder ein entsprechender kompatibler Prozessor)
- 64 MB Arbeitsspeicher.

Unter Microsoft Windows 2000 Professional (Service Pack 3 oder höher), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 oder höher), Microsoft Windows XP Professional x64 Edition:

- Prozessor Intel Pentium 300 MHz oder höher (oder ein entsprechender kompatibler Prozessor)
- 128 MB Arbeitsspeicher.

Microsoft Windows Vista, Microsoft Windows Vista x64:

- Prozessor Intel Pentium 800 MHz 32-Bit (x86) / 64-Bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor)
- 512 MB Arbeitsspeicher.

2.4. Lieferumfang

Kaspersky Internet Security kann bei unseren Vertriebspartnern (als verpackte Variante) oder in einem Online-Shop (z.B. www.kaspersky.com/de, Abschnitt **E-Store**) erworben werden.

Wenn Sie das Produkt als verpackte Variante erwerben, umfasst der Lieferumfang des Softwareprodukts die folgenden Elemente:

- Versiegelter Umschlag mit Installations-CD, auf der die Dateien der Software gespeichert sind.
- Benutzerhandbuch
- Code zur Programmaktivierung (auf dem Umschlag mit der Installations-CD aufgeklebt).
- Lizenzvertrag.

Bitte lesen Sie vor der Installation sorgfältig den Lizenzvertrag im Anhang des Handbuchs.

Beim Kauf von Kaspersky Internet Security in einem Online-Shop kopieren Sie das Produkt von der Kaspersky-Lab-Webseite (Abschnitt **Downloads** → **Produkte herunterladen**). Das Benutzerhandbuch kann aus dem Abschnitt **Downloads** → **Dokumentationen** heruntergeladen werden.

Der Aktivierungscode wird Ihnen nach Eingang der Bezahlung per E-Mail zugeschickt.

Der Lizenzvertrag ist eine rechtsgültige Vereinbarung zwischen Ihnen und Kaspersky Lab Ltd., in der festgelegt wird, zu welchen Bedingungen Sie das von Ihnen erworbene Softwareprodukt verwenden dürfen.

Bitte lesen Sie den Lizenzvertrag sorgfältig!

Durch das Öffnen der versiegelten Packung mit der Installations-CD (oder Disketten) stimmen Sie allen Bedingungen des Lizenzvertrags zu.

2.5. Service für registrierte Benutzer

Kaspersky Lab bietet seinen legalen Benutzern ein breites Spektrum an Serviceleistungen, die eine gesteigerte Effektivität von Kaspersky Internet Security ermöglichen.

Durch die Aktivierung des Programms werden Sie zum registrierten Programmbenutzer und können während des Zeitraums der Lizenzgültigkeit folgende Dienste in Anspruch nehmen:

- Nutzung neuer Versionen der betreffenden Software
- Beratung bei Fragen zu Installation, Konfiguration und Benutzung der betreffenden Software (per Telefon und E-Mail)
- Nachrichten über das Erscheinen neuer Software von Kaspersky Lab und über das Auftauchen neuer Viren (Dieser Service gilt für Benutzer, die den Newsletter von Kaspersky Lab abonniert haben).

Die Beratung bezieht sich nicht auf Fragen über Funktion und Benutzung von Betriebssystemen und anderen Technologien.

KAPITEL 3. INSTALLATION VON KASPERSKY INTERNET SECURITY 6.0

Kaspersky Internet Security kann vollständig oder teilweise auf Ihrem Computer installiert werden.

Bei teilweiser Installation können Sie die zu installierenden Komponenten auswählen. Nicht installierte Programmkomponenten können später installiert werden. Allerdings wird dazu die ursprüngliche Distribution benötigt. Deshalb wird empfohlen, die Distributionsdatei des Programms auf die Festplatte Ihres Computers zu kopieren.

Die Anwendung kann auf folgende Weise installiert werden:

- mit Hilfe des Installationsassistenten (s. Pkt. 3.1 auf S. 34)
- aus der Befehlszeile (s. Pkt. 3.3 auf S. 50).

3.1. Installation mit Hilfe des Installationsassistenten

Es wird empfohlen, alle laufenden Anwendungen zu beenden, bevor mit der Installation von Kaspersky Internet Security begonnen wird.

Um Kaspersky Internet Security auf Ihrem Computer zu installieren, starten Sie die Distributionsdatei von der Installations-CD.

Hinweis.

Die Installation der Anwendung von einer Distribution, die aus dem Internet heruntergeladen wurde, stimmt vollständig mit der Installation der Anwendung von einer Distributions-CD überein.

Das Installationsprogramm funktioniert im Dialogmodus. Jedes Dialogfenster enthält eine Auswahl von Schaltflächen zur Steuerung des Installationsprozesses. Unten finden Sie die Funktionsbeschreibung der wichtigsten Schaltflächen:

- **Weiter >** – Aktion bestätigen und zum folgenden Schritt des Installationsvorgangs weitergehen.
- **< Zurück** – zum vorherigen Installationsschritt zurückkehren.
- **Abbrechen** – Installation des Produkts abbrechen.
- **Fertig stellen** – Installationsprozedur des Programms auf dem Computer fertig stellen.

Betrachten wir die einzelnen Schritte des Installationsvorgangs ausführlich:

Schritt 1. Überprüfen des Systems auf die Installationsvoraussetzungen für Kaspersky Internet Security

Bevor das Programm auf Ihrem Computer installiert wird, werden das installierte Betriebssystem und die vorhandenen Service Packs auf Übereinstimmung mit den Softwarevoraussetzungen für die Installation von Kaspersky Internet Security überprüft. Außerdem wird überprüft, ob die erforderlichen Programme auf Ihrem Computer vorhanden sind und ob Sie über die notwendigen Rechte zur Programminstallation verfügen.

Sollte eine bestimmte Voraussetzung nicht erfüllt sein, dann erscheint eine entsprechende Meldung auf dem Bildschirm. Es wird empfohlen, vor der Installation von Kaspersky Internet Security die erforderlichen Programme und mit Hilfe des Diensts **Windows Update** die fehlenden Service Packs zu installieren.

Schritt 2. Startfenster des Installationsvorgangs

Wenn Ihr System die Voraussetzungen vollständig erfüllt, erscheint sofort nach dem Start der Distributionsdatei auf dem Bildschirm das Startfenster, das Informationen über den Beginn der Installation von Kaspersky Internet Security auf Ihrem Computer enthält.

Klicken Sie auf **Weiter >**, um die Installation fortzusetzen, oder klicken Sie auf **Abbrechen**, um die Installation des Produkts zu abzubrechen.

Schritt 3. Lesen des Lizenzvertrags

Das folgende Fenster des Installationsprogramms enthält den Lizenzvertrag zwischen Ihnen und Kaspersky Lab. Bitte lesen Sie den Vertrag aufmerksam. Wenn Sie allen Punkten des Vertrags zustimmen, wählen Sie die Variante **Ich akzeptiere die Bedingungen des Lizenzvertrags** und klicken Sie auf die Schaltfläche **Weiter**. Die Installation wird fortgesetzt.

Schritt 4. Auswahl des Installationsordners

Im nächsten Schritt der Installation von Kaspersky Internet Security wird festgelegt, in welchem Ordner Ihres Computers das Produkt installiert werden soll. Der standardmäßige Pfad lautet: **<Laufwerk>\Programme\Kaspersky Lab\Kaspersky Internet Security 6.0**.

Sie können einen anderen Ordner wählen. Klicken Sie dazu auf die Schaltfläche **Durchsuchen** und wählen Sie den Ordner im Standardfenster zur Ordnerauswahl aus oder geben Sie den Pfad des Ordners im entsprechenden Eingabefeld an.

> Falls Sie den Pfad manuell eingeben, beachten Sie, dass der vollständige Name des Installationsordners aus maximal 200 Zeichen bestehen und keine Sonderzeichen enthalten darf.

Klicken Sie auf die Schaltfläche **Weiter**, um die Installation fortzusetzen.

Schritt 5. Auswahl des Installationstyps

Hier können Sie auswählen, in welchem Umfang das Programm auf Ihrem Computer installiert werden soll. Drei Installationsvarianten sind vorgesehen:

Vollständig. In diesem Fall werden alle Komponenten von Kaspersky Internet Security auf Ihrem Computer installiert. Die weitere Abfolge der Installationsschritte wird in Schritt 7 beschrieben.

Benutzerdefiniert. In diesem Fall wird Ihnen angeboten, die Programmkomponenten auszuwählen, die auf Ihrem Computer installiert werden sollen. Details siehe Schritt 6.

Antivirenschutzkomponenten. Bei Auswahl dieser Variante werden nur die Komponenten installiert, die den Virenschutz Ihres Computers gewährleisten. Die Komponenten Anti-Hacker, Anti-Spam und Anti-Spy werden nicht installiert.

Klicken Sie zur Auswahl eines Installationstyps auf die entsprechende Schaltfläche.

Schritt 6. Auswahl der zu installierenden Programmkomponenten

> Dieser Schritt wird nur ausgeführt, wenn Sie die **benutzerdefinierte** Installation des Programms auf Ihrem Computer gewählt haben.

Bei der benutzerdefinierten Installation muss eine Liste der Komponenten von Kaspersky Internet Security festgelegt werden, die installiert werden sollen. Standardmäßig sind alle Virenschutzkomponenten und die Komponente zur

Virensuche gewählt. Anti-Hacker, Anti-Spam und Anti-Spy werden nicht installiert.

Um eine Komponente zur anschließenden Installation auszuwählen, wird durch Rechtsklick auf das Symbol neben dem Komponentennamen das Kontextmenü geöffnet und der Punkt **Die Komponente wird auf der lokalen Festplatte installiert** gewählt. Eine Beschreibung des Schutzes, den die betreffende Komponente gewährleistet und Informationen über den für ihre Installation auf der Festplatte erforderlichen Platz befinden sich im unteren Bereich dieses Fensters der Programminstallation.

Um die Installation einer Komponente abzulehnen, wählen Sie im Kontextmenü den Punkt **Die Komponente wird nicht verfügbar sein**. Beachten Sie, dass Sie auf den Schutz vor einer ganzen Reihe gefährlicher Programme verzichten, wenn Sie eine bestimmte Komponente nicht installieren.

Klicken Sie auf die Schaltfläche **Weiter**, nachdem Sie die zu installierenden Komponenten gewählt haben. Um zur Liste der standardmäßig zu installierenden Komponenten zurückzukehren, klicken Sie auf die Schaltfläche **Zurücksetzen**.

Schritt 7. Deaktivieren der Microsoft Windows Firewall

Dieser Schritt wird nur ausgeführt, wenn Kaspersky Internet Security auf einem Computer mit laufender Firewall installiert wird und die Komponente Anti-Hacker zur Installation ausgewählt wurde.

In diesem Schritt der Installation von Kaspersky Internet Security wird Ihnen angeboten, die Firewall des Betriebssystems Microsoft Windows zu deaktivieren, weil die zu Kaspersky Internet Security gehörende Komponente Anti-Hacker den umfassenden Schutz Ihrer Arbeit im Netzwerk gewährleistet und ein zusätzlicher Schutz durch Mittel des Betriebssystems nicht erforderlich ist.

Wenn Sie Anti-Hacker als Firewall verwenden möchten, klicken Sie auf die Schaltfläche **Weiter**. Die Firewall von Microsoft Windows wird in diesem Fall automatisch deaktiviert.

Wenn Sie Ihren Computer mit Hilfe der Firewall von Microsoft Windows schützen möchten, wählen Sie die Variante **Firewall von Microsoft Windows verwenden**. Die Komponente Anti-Hacker wird in diesem Fall zwar installiert, zur Vermeidung von Konflikten bei der Arbeit des Programms aber deaktiviert.

Schritt 8. Suche anderer Antiviren-Programme

Auf dieser Etappe erfolgt die Suche nach anderen Antiviren-Produkten (einschließlich Kaspersky-Lab-Produkte), die auf Ihrem Computer installiert sind

und deren gemeinsame Verwendung mit Kaspersky Internet Security zu Konflikten führen kann.

Wenn auf Ihrem Computer solche Programme gefunden werden, werden Sie auf dem Bildschirm aufgelistet. Sie werden aufgefordert, diese Programme zu löschen, bevor die Installation fortgesetzt wird.

Unter der Liste der gefundenen Antiviren-Anwendungen können Sie wählen, ob diese automatisch oder manuell entfernt werden sollen.

Wenn sich unter den gefundenen Antiviren-Programmen die Anwendung Kaspersky Anti-Virus Personal oder Kaspersky Anti-Virus Personal Pro befindet, wird empfohlen, vor der Deinstallation den bei der Arbeit dieser Programme verwendeten Lizenzschlüssel zu speichern. Sie können ihn als Schlüssel für Kaspersky Internet Security 6.0 verwenden. Außerdem wird empfohlen, die Quarantäne- und Backup-Objekte zu speichern. Diese Objekte werden automatisch in die entsprechenden Speicher von Kaspersky Internet Security verschoben und Sie können damit weiterarbeiten.

Klicken Sie auf die Schaltfläche **Weiter**, um die Installation fortzusetzen.

Schritt 9. Abschlussvorbereitungen für die Programminstallation

Nun wird Ihnen angeboten, die Programminstallation auf Ihrem Computer abschließend vorzubereiten. Sie können festlegen, ob bei der Arbeit des Programms vorhandene Schutzeinstellungen, Bedrohungssignaturen und die Anti-Spam-Wissensdatenbank verwendet werden sollen, wenn solche auf Ihrem Computer bei der Deinstallation einer älteren Version von Kaspersky Internet Security gespeichert worden sind (wenn Sie beispielsweise die Beta-Version installiert hatten und jetzt eine kommerzielle Version des Programms installieren).

Im Folgenden wird beschrieben, wie die Verwendung der oben genannten Optionen aktiviert wird.

Wenn auf Ihrem Computer bereits eine ältere Version von Kaspersky Internet Security installiert war und bei der Deinstallation die Bedrohungssignaturen auf dem Computer gespeichert wurden, können Sie diese in der zu installierenden Version verwenden. Aktivieren Sie dazu das Kontrollkästchen ☑ **Bedrohungssignaturen**. Die Bedrohungssignaturen, die in der Programmdistribution enthalten sind, werden dann nicht auf Ihren Computer kopiert.

Um die Schutzparameter zu verwenden, die Sie in der vorherigen Version eingestellt und auf dem Computer gespeichert haben, aktivieren Sie das Kontrollkästchen ☑ **Schutzeinstellungen**.

Es wird außerdem empfohlen, die Wissensdatenbank von Anti-Spam zu verwenden, wenn diese bei der Deinstallation der vorherigen Programmversion

gespeichert wurde. Dadurch wird das erneute Training von Anti-Spam überflüssig. Um die bereits von Ihnen erstellte Wissensdatenbank zu berücksichtigen, aktivieren Sie das Kontrollkästchen ☑ **Anti-Spam-Wissensdatenbank**.

Bei der Erstinstallation von Kaspersky Internet Security 6.0 sollte das Kontrollkästchen ☑ **Schutz für Module vor der Installation aktivieren** nicht entfernt werden. Der aktivierte Modulschutz erlaubt, falls während der Anwendungsinstallation Fehler auftreten, die Installation auf korrekte Weise rückgängig zu machen. Bei einem wiederholten Versuch zur Installation der Anwendung wird empfohlen, dieses Kontrollkästchen zu entfernen.

> Wird die Anwendung im entfernten Modus über **Windows Remote Desktop** auf dem Computer installiert, dann wird empfohlen, das Kontrollkästchen ☑ **Schutz für Module vor der Installation aktivieren** zu deaktivieren. Andernfalls besteht die Möglichkeit, dass der Installationsvorgang nicht oder fehlerhaft durchgeführt wird.

Klicken Sie auf die Schaltfläche **Weiter**, um die Installation fortzusetzen.

Schritt 10. Abschluss des Installationsvorgangs

Das Fenster **Installation wird abgeschlossen** enthält Informationen über den Abschluss des Installationsprozesses von Kaspersky Internet Security auf Ihrem Computer.

Wenn zum Fertigstellen der Programminstallation der Neustart des Computers erforderlich ist, erscheint eine entsprechende Meldung auf dem Bildschirm. Nach dem Neustart des Systems wird automatisch der Konfigurationsassistent für Kaspersky Internet Security gestartet.

Wenn zum Fertigstellen der Installation kein Systemneustart erforderlich ist, klicken Sie auf die Schaltfläche **Weiter**, um zum Konfigurationsassistenten des Programms zu wechseln.

3.2. Konfigurationsassistent

Der Konfigurationsassistent für Kaspersky Internet Security 6.0 wird am Ende der Programminstallation gestartet. Seine Aufgabe ist es, Sie bei der ersten Konfiguration der Programmeinstellungen zu unterstützen und dabei die Besonderheiten der Aufgaben Ihres Computers zu berücksichtigen.

Der Konfigurationsassistent besitzt das Aussehen eines Microsoft Windows-Programmassistenten (Windows Wizard) und besteht aus einer Folge von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die

Schaltflächen **Weiter** und **Zurück**, zum Abschluss des Assistenten klicken Sie auf die Schaltfläche **Fertig stellen**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Sie können die Etappen des Konfigurationsassistenten bei der Programminstallation überspringen, indem Sie das Assistentenfenster schließen. Der Assistent kann später über die Programmoberfläche gestartet werden, wenn die ursprünglichen Schutzeinstellungen von Kaspersky Internet Security wiederhergestellt werden (s. Pkt. 17.13 auf S. 308).

3.2.1. Verwendung von Objekten, die in Version 5.0 gespeichert wurden

Dieses Fenster des Assistenten erscheint, wenn die Anwendung über Kaspersky Anti-Virus Version 5.0 installiert wird. Ihnen wird angeboten, die Daten, die von Version 5.0 verwendet wurden und auf Version 6.0 übertragen werden sollen, auszuwählen. Dazu gehören Quarantäne- und Backup-Objekte sowie Schutzeinstellungen.

Aktivieren Sie die entsprechenden Kontrollkästchen, um diese Daten in Version 6.0 zu verwenden.

3.2.2. Aktivierung des Programms

Der Aktivierungsvorgang des Programms besteht in der Installation eines Lizenzschlüssels, auf dessen Grundlage das Programm Kaspersky Internet Security das Vorhandensein einer Lizenz überprüft und deren Gültigkeitsdauer ermittelt.

Der Lizenzschlüssel enthält Dienstinformationen, die für die volle Funktionsfähigkeit des Programms erforderlich sind, sowie zusätzliche Angaben:

- Informationen über den Support (von wem und wo man technische Unterstützung erhalten kann).
- Bezeichnung, Nummer und Gültigkeitsende der Lizenz.

> Achtung!
>
> Um das Programm zu aktivieren, ist eine Internetverbindung notwendig. Ist im Augenblick der Installation keine Internetverbindung vorhanden, dann kann die Aktivierung später über die Programmoberfläche erfolgen (s. Pkt. 17.5 auf S. 283).

3.2.2.1. Auswahl der Aktivierungsmethode

Abhängig davon, ob Sie über einen Lizenzschlüssel für das Programm Kaspersky Internet Security verfügen oder ihn von einem Kaspersky-Lab-Server erhalten müssen, bestehen mehrere Möglichkeiten zur Aktivierung des Programms:

- **Mit Aktivierungscode aktivieren**. Wählen Sie diese Aktivierungsmethode, wenn Sie eine kommerzielle Programmversion erworben haben und Sie einen Aktivierungscode erhalten haben. Auf Basis dieses Codes bekommen Sie einen Lizenzschlüssel, der Ihnen den Zugriff auf die volle Funktionsfähigkeit des Programms während der gesamten Gültigkeitsdauer der Lizenz bietet.
- **Testversion aktivieren**. Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Sie erhalten einen kostenlosen Lizenzschlüssel, dessen Gültigkeitsdauer durch die Lizenz der Testversion dieser Anwendung beschränkt ist.
- **Vorherigen Lizenzschlüssel verwenden**. Aktivieren Sie die Anwendung mit Hilfe einer bereits vorhandenen Lizenzschlüsseldatei für Kaspersky Internet Security 6.0.
- **Das Programm später aktivieren**. Bei der Auswahl dieser Variante wird die Aktivierung des Programms übersprungen. Kaspersky Internet Security 6.0 wird auf Ihrem Computer installiert und Sie können alle Programmfunktionen außer dem Update nutzen (Die Bedrohungssignaturen können nur einmal nach der Programminstallation aktualisiert werden).

Wenn die erste oder zweite der oben genannten Varianten gewählt wird, erfolgt die Aktivierung der Anwendung über einen Kaspersky-Lab-Webserver. Für die Verbindung mit diesem Server ist eine Internetverbindung erforderlich. Vor Beginn der Aktivierung sollten die Parameter für die Netzwerkverbindung (s. Pkt. 16.4.3 auf S. 251) im Fenster, das mit der Schaltfläche **LAN-Einstellungen** geöffnet wird, überprüft und bei Bedarf geändert werden. Wenden Sie sich an Ihren Systemadministrator oder Internetprovider, um genauere Informationen über die Netzwerkparameter zu erhalten.

3.2.2.2. Eingabe des Aktivierungscodes

Zur Aktivierung des Programms ist die Eingabe des Aktivierungscodes erforderlich, den Sie auf der beiliegenden Registrierungskarte finden. Der Code muss mit lateinischen Zeichen eingegeben werden.

Sie können im unteren Bereich des Fensters freiwillig Ihre Kontaktinformationen angeben: Familienname, Name, E-Mail-Adresse, Land und Wohnort. Diese

Informationen können zur Identifikation eines registrierten Benutzers erforderlich sein, wenn beispielsweise ein Schlüssel verloren geht oder gestohlen wird. In diesem Fall können Sie auf Basis der Kontaktinformationen einen anderen Lizenzschlüssel erhalten.

3.2.2.3. Download des Lizenzschlüssels

Der Konfigurationsassistent baut eine Verbindung mit den Kaspersky-Lab-Servern im Internet auf und sendet Ihre Anmeldungsdaten (Aktivierungscode, Kontaktinformationen) zur Überprüfung an den Server.

Bei erfolgreicher Überprüfung des Aktivierungscodes erhält der Assistent eine Lizenzschlüsseldatei. Wenn Sie eine Testversion des Programms installieren, erhält der Konfigurationsassistent ohne Aktivierungscode einen Testschlüssel.

Die empfangene Datei wird automatisch für die Arbeit mit dem Programm installiert und das letzte Fenster des Assistenten, das ausführliche Angaben über die Lizenz enthält, informiert Sie über den Abschluss der Aktivierung.

Wenn der Aktivierungscode die Überprüfung nicht besteht, erscheint ein entsprechender Hinweis auf dem Bildschirm. Wenden Sie sich in diesem Fall an die Firma, bei der Sie das Programm erworben haben.

3.2.2.4. Auswahl einer Lizenzschlüsseldatei

Wenn Sie bereits eine Lizenzschlüsseldatei für das Programm Kaspersky Internet Security 6.0 besitzen, bietet Ihnen der Assistent in diesem Fenster an, den Schlüssel zu installieren. Verwenden Sie dazu die Schaltfläche **Durchsuchen** und wählen Sie im Standardfenster zur Dateiauswahl eine Datei mit der Endung *.key* aus.

Nach der erfolgreichen Installation des Schlüssels erscheinen im unteren Bereich des Fensters Informationen über die Lizenz: Name des Besitzers, Nummer und Typ (kommerzielle, für Beta-Test, Test usw.) der Lizenz, Gültigkeitsende der Lizenz.

3.2.2.5. Abschluss der Programmaktivierung

Der Konfigurationsassistent informiert Sie über den erfolgreichen Abschluss der Programmaktivierung. Außerdem werden Informationen über den installierten Lizenzschlüssel angezeigt: Name des Besitzers, Nummer und Typ (kommerzielle, für Beta-Test, Test usw.) der Lizenz, Gültigkeitsende der Lizenz.

3.2.3. Auswahl des Schutzmodus

In diesem Fenster des Konfigurationsassistenten wird Ihnen angeboten, den Schutzmodus zu wählen, in dem die Anwendung arbeiten soll:

Basisschutz. Dieser Modus gilt als Standard und ist für die meisten Benutzer geeignet, die über begrenzte Erfahrung mit Computern und Antivirenprodukten verfügen. In diesem Modus funktionieren die Anwendungskomponenten auf der empfohlenen Schutzstufe und der Benutzer wird nur über das Eintreten gefährlicher Ereignisse (z.B. Fund eines schädlichen Objekts, Ausführen gefährlicher Aktionen) informiert.

Interaktiver Schutz. Dieser Modus bietet im Vergleich zum Basisschutz einen erweiterten Schutz für die Daten auf dem Computer. Er erlaubt die Kontrolle über Versuche zum Verändern von Systemeinstellungen, über verdächtige Aktivität im System und unerlaubte Aktionen im Netzwerk. Alle oben genannten Aktionen können sowohl das Ergebnis der Aktivität schädlicher Programme, als auch standardmäßige Aktionen im Rahmen der Arbeit von auf Ihrem Computer verwendeten Programmen sein. Sie müssen in jedem konkreten Fall entscheiden, ob eine Aktion erlaubt oder unzulässig ist.

Wenn Sie diesen Modus wählen, dann geben Sie an, in welchen Fällen er verwendet werden soll:

- ☑ **Anti-Hacker-Trainingsmodus aktivieren** – Wenn Programme, die auf Ihrem Computer installiert sind, versuchen, eine Verbindung mit Netzwerkressourcen aufzubauen, wird der Benutzer aufgefordert, die Aktionen zu bestätigen. Sie können die Verbindung erlauben oder verbieten, und für das betroffene Programm eine Anti-Hacker-Regel erstellen. Wenn der Trainingsmodus nicht aktiviert wird, arbeitet Anti-Hacker im Modus Minimaler Schutz, in dem allen Anwendungen der Zugriff auf Netzwerkressourcen erlaubt wird.
- ☑ **Überwachung der Systemregistrierung aktivieren** – Bei Versuchen zum Ändern von Systemregistrierungsobjekten erfolgt eine Bestätigungsabfrage.

> Wenn die Anwendung auf einem Computer mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64 installiert ist, sind die unten genannten Parameter für den interaktiven Modus nicht vorhanden.

- ☑ **Integritätskontrolle für Anwendungen aktivieren** – Wenn versucht wird, Module in die zu kontrollierenden Anwendungen zu laden, erfolgt eine Bestätigungsabfrage.
- ☑ **Den erweiterten Proaktiven Schutz aktivieren** – Die Analyse aller verdächtigen Aktivitäten von Anwendungen im System wird

aktiviert. Dazu zählen auch Browserstart mit Befehlzeilenschlüsseln, Eindringen in Programmprozesse und Eindringen von Fenster-Hooks (diese Parameter sind standardmäßig deaktiviert).

3.2.4. Konfiguration der Update-Einstellungen

Die Qualität des Schutzes Ihres Computers ist direkt vom rechtzeitigen Download der Updates für die Bedrohungssignaturen und Programm-Module abhängig. In diesem Fenster des Assistenten wird Ihnen angeboten, den Modus für das Programmupdate zu wählen und Einstellungen für den Zeitplan vorzunehmen:

- **Automatisch**. Kaspersky Internet Security prüft in festgelegten Zeitabständen, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Virusepidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates vorhanden sind, lädt die Anwendung sie herunter und installiert sie auf dem Computer. Dieser Modus gilt als Standard.
- **Alle ... Tage um 15:00** (Das Intervall kann in Abhängigkeit von den Zeitplaneinstellungen variieren). Das Update wird automatisch nach dem festgelegten Zeitplan gestartet. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.
- **Manuell**. In diesem Fall starten Sie das Programmupdate selbständig.

Beachten Sie, dass die Datenbanken mit den Bedrohungssignaturen und die Programm-Module, die in der Distribution enthalten sind, zum Zeitpunkt der Programminstallation bereits veraltet sein können. Wir empfehlen deshalb, die aktuellen Programmupdates herunterzuladen. Klicken Sie dazu auf die Schaltfläche **Jetzt aktualisieren**. In diesem Fall empfängt Kaspersky Internet Security die erforderlichen Updates von den Updateseiten im Internet und installiert sie auf Ihrem Computer.

Wenn Sie die Updateparameter anpassen möchten (Netzwerkparameter festlegen, die Ressource wählen, von der das Update erfolgt, den am nächsten bei Ihrem Standort liegenden Updateserver wählen), klicken Sie auf die Schaltfläche **Einstellungen**.

3.2.5. Konfiguration des Zeitplans für die Virenuntersuchung

Die Suche von schädlichen Objekten in vorgegebenen Untersuchungsbereichen ist eine der wichtigsten Aufgaben, die den Schutz Ihres Computers gewährleistet.

Bei der Installation von Kaspersky Internet Security werden standardmäßig drei Untersuchungsaufgaben erstellt. In diesem Fenster bietet Ihnen der Assistent an, den Startmodus für die Untersuchungsaufgaben festzulegen:

Autostart-Objekte untersuchen

Standardmäßig findet die Untersuchung der Autostart-Objekte automatisch bei jedem Start von Kaspersky Internet Security statt. Die Zeitplaneinstellungen können im Fenster angepasst werden, das mit der Schaltfläche **Ändern** geöffnet wird.

Kritische Bereiche untersuchen

Aktivieren Sie das Kontrollkästchen im entsprechenden Block, damit die Virenuntersuchung der kritischen Computerbereiche (Systemspeicher, Autostart-Objekte, Bootsektoren, Microsoft Windows-Systemverzeichnisse) automatisch gestartet wird. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.

Der automatische Start dieser Aufgabe ist standardmäßig deaktiviert.

Vollständig Untersuchung des Computers

Aktivieren Sie das Kontrollkästchen im entsprechenden Block, damit die vollständige Untersuchung Ihres Computers auf Viren automatisch gestartet wird. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.

Der automatische Start dieser Aufgabe nach Zeitplan ist standardmäßig deaktiviert. Wir empfehlen aber, sofort nach der Programminstallation die vollständige Virenuntersuchung des Computers zu starten.

3.2.6. Zugriffsbegrenzung für die Anwendung

Da ein PC von mehreren Personen benutzt werden kann, die über ein unterschiedliches Maß an Fertigkeiten im Umgang mit Computern verfügen, und weil die Gefahr besteht, dass Schadprogramme versuchen, den Schutz Ihres

Computers auszuschalten, bietet Kaspersky Internet Security die Möglichkeit, den Zugriff auf die Anwendung mit Hilfe eines Kennworts zu beschränken. Der Kennwortschutz erlaubt es, die Anwendung vor Versuchen zum unerlaubten Abschalten des Schutzes und zum Ändern der Einstellungen zu schützen.

Um den Kennwortschutz zu verwenden, aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren** und füllen Sie die Felder **Kennwort** und **Kennwort bestätigen** aus.

Geben Sie darunter den Bereich an, auf den sich die Zugriffsbeschränkung beziehen soll:

Alle Operationen (außer Gefahrenmeldungen). Bei einer beliebigen Aktion des Benutzers mit der Anwendung wird das Kennwort abgefragt. Eine Ausnahme bildet die Arbeit mit Hinweisen über den Fund gefährlicher Objekte.

Nur für ausgewählte Operationen:

- **Veränderungen von Programmeinstellungen** – Wenn der Benutzer versucht, geänderte Anwendungseinstellungen zu speichern, wird das Kennwort abgefragt.
- **Programm beenden** – Wenn der Benutzer versucht, die Anwendung zu beenden, wird das Kennwort abgefragt.
- **Schutzkomponenten und Untersuchungsaufgaben anhalten/ beenden** – Das Kennwort wird abgefragt, wenn der Benutzer versucht, die Arbeit einer beliebigen Schutzkomponente oder einer Untersuchungsaufgabe anzuhalten oder zu beenden.

3.2.7. Integritätskontrolle für Anwendungen

Auf dieser Etappe des Assistenten analysiert Kaspersky Internet Security die auf Ihrem Computer installierten Anwendungen (dynamische Bibliotheksdateien, digitale Herstellersignaturen), berechnet die Kontrollsummen der Anwendungsdateien und erstellt eine Liste der im Hinblick auf die Antivirensicherheit vertrauenswürdigen Programme. In diese Liste werden beispielsweise automatisch alle Anwendungen aufgenommen, die eine Signatur der Microsoft Corporation besitzen.

Die bei der Strukturanalyse der Anwendungen ermittelten Informationen werden danach von der Anwendung Kaspersky Internet Security verwendet, um das Eindringen von schädlichem Code in Anwendungsmodule zu verhindern.

Die Analyse der auf Ihrem Computer installierten Anwendungen kann eine gewisse Zeit in Anspruch nehmen.

3.2.8. Konfiguration der Firewall Anti-Hacker

Anti-Hacker ist eine Programmkomponente von Kaspersky Internet Security, die für die Sicherheit Ihres Computers in lokalen Netzwerken und im Internet verantwortlich ist. In diesem Schritt des Konfigurationsassistenten wird Ihnen angeboten, eine Auswahl von Regeln zu erstellen, die Anti-Hacker bei der Analyse der Netzwerkaktivität auf Ihrem Computer verwenden wird.

3.2.8.1. Festlegen des Status der Sicherheitszone

Auf dieser Etappe analysiert der Konfigurationsassistent die Netzwerkumgebung Ihres Computers. Aufgrund der Analyseergebnisse wird die gesamte Netzwerkumgebung in bedingte Zonen unterteilt:

Internet – globales Netzwerk Internet. In dieser Zone arbeitet Kaspersky Internet Security als Personal Firewall. Dabei wird die gesamte Netzwerkaktivität durch Regeln für Pakete und Anwendungen geregelt, die in der Grundeinstellung maximale Sicherheit gewährleisten. Die Schutzbedingungen bei der Arbeit in dieser Zone können nicht geändert werden. Zur Steigerung der Sicherheit kann der Stealth-Modus aktiviert werden.

Sicherheitszonen – verschiedene bedingte Zonen, die teilweise mit Subnetzen übereinstimmen, zu denen der Computer gehört (auch lokale Netzwerke zu Hause oder bei der Arbeit). Diese Zonen werden standardmäßig als Zonen mit mittlerer Risikostufe betrachtet. Sie können den Status dieser Zonen in Abhängigkeit der Vertrauenswürdigkeit des jeweiligen Subnetzes ändern, sowie die Regeln für Pakete und Anwendung anpassen.

Alle gefundenen Zonen werden in einer Liste angezeigt. Für jede Zone werden eine Beschreibung, die Subnetzadresse und -maske sowie der Status, auf dessen Grundlage eine bestimmte Netzwerkaktivität erlaubt oder verboten wird, genannt:

- **Internet**. Dieser Status wird standardmäßig dem Internet zugeordnet, weil der Computer im Internet allen möglichen Typen von Bedrohungen unterliegt. Die Auswahl dieses Status wird außerdem für Netzwerke empfohlen, die nicht durch Antiviren-Anwendungen, Firewalls, Filter usw. geschützt werden. Bei der Auswahl dieses Status wird die maximale Sicherheit der Arbeit des Computers in dieser Zone gewährleistet. Das bedeutet:

- Jede beliebige netzwerkbezogene NetBios-Aktivität im Rahmen des Subnetzes wird blockiert.
- Das Ausführen von Regeln für Anwendungen und Pakete, die eine netzwerkbezogene NetBios-Aktivität im Rahmen dieses Subnetzes erlauben, wird verboten.

Selbst wenn Sie einen gemeinsamen Ordner erstellt haben, besitzen die Benutzer eines Subnetzes mit diesem Status keinen Zugriff auf die darin enthaltenen Informationen. Außerdem haben Sie bei Auswahl dieses Status keinen Zugriff auf Dateien und Drucker auf anderen Computern des Netzwerks.

- **Lokales Netzwerk**. Dieser Status wird standardmäßig der Mehrzahl der Sicherheitszonen zugewiesen, die bei der Analyse der Netzwerkumgebung des Computers gefunden werden. Eine Ausnahme bildet das Internet. Es wird empfohlen, diesen Status für Zonen mit mittlerer Risikostufe zu verwenden (beispielsweise für ein lokales Firmennetzwerk). Bei der Auswahl dieses Status wird erlaubt:
  - jede beliebige netzwerkbezogene NetBios-Aktivität im Rahmen des Subnetzes.
  - das Ausführen von Regeln für Anwendungen und Pakete, die eine netzwerkbezogene NetBios-Aktivität im Rahmen dieses Subnetzes erlauben.

  Wählen Sie diesen Status, wenn Sie Zugriff auf bestimmte Verzeichnisse oder Drucker Ihres Computers gewähren, aber jede andere externe Aktivität verbieten möchten.

- **Vertrauenswürdig**. Es wird empfohlen, diesen Status nur für eine Zone zu verwenden, die Ihrer Meinung nach absolut sicher ist und in der dem Computer bei der Arbeit weder Angriffe noch Versuche zu unerlaubtem Datenzugriff drohen. Bei der Auswahl dieses Status wird jede beliebige Netzwerkaktivität erlaubt. Selbst wenn Sie die Stufe Maximaler Schutz gewählt und Verbotsregeln erstellt haben, gelten diese nicht für entfernte Computer eines vertrauenswürdigen Netzwerks.

Für ein Netzwerk mit dem Status **Internet** können Sie zur Erhöhung der Sicherheit den *Stealth-Modus* verwenden. In diesem Modus wird nur die die von Ihrem Computer initiierte Netzwerkaktivität erlaubt. Praktisch bedeutet das, dass Ihr Computer für die externe Umgebung "unsichtbar" wird. Gleichzeitig beeinträchtigt der Modus aber Ihre Arbeit im Internet in keiner Weise.

Es wird davor gewarnt, den Stealth-Modus zu verwenden, wenn der Computer als Server dient (beispielsweise als Mailserver oder http-Server). Andernfalls können Computer, die sich an den Server wenden, diesen im Netzwerk nicht finden.

Um den Status einer Zone zu ändern oder den Stealth-Modus zu aktivieren bzw. deaktivieren, wählen Sie die die Zone in der Liste aus und verwenden Sie die entsprechenden Links im Block **Beschreibung**, der sich unterhalb der Liste befindet. Diese Aktionen können auch im Fenster **Parameter der Zone** vorgenommen werden, das mit der Schaltfläche **Ändern** geöffnet wird. In diesem Fenster können auch Adresse und Maske des Subnetzes geändert werden.

Mit der Schaltfläche **Suchen** können Sie der Liste eine neue Zone hinzufügen. In diesem Fall sucht Anti-Hacker nach verfügbaren Zonen. Wenn solche Zonen gefunden werden, wird Ihnen angeboten, deren Status festzulegen. Daneben können Sie einen neue Zone auch manuell zur Liste hinzufügen (beispielsweise wenn Sie ein Notebook an ein neues Netzwerk anschließen). Verwenden Sie dazu die Schaltfläche **Hinzufügen** und geben Sie im Fenster **Parameter der Zone** die erforderlichen Informationen an.

Um ein Netzwerk aus der Liste zu löschen, verwenden Sie die Schaltfläche **Löschen**.

3.2.8.2. Erstellen einer Liste der Netzwerkanwendungen

Der Konfigurationsassistent analysiert die auf Ihrem Computer installierte Software und erstellt eine Liste der Anwendungen, die für ihre Arbeit ein Netzwerk verwenden.

Anti-Hacker erstellt für jede dieser Anwendungen eine Regel, welche die Netzwerkaktivität steuert. Die Regeln beruhen auf den von Kaspersky Lab erstellten und im Lieferumfang des Produkts enthaltenen Vorlagen für die gebräuchlichsten Anwendungen, die Netzwerke verwenden.

Die Liste der Netzwerkanwendungen und die dafür erstellten Regeln können Sie im Konfigurationsfenster von Anti-Hacker anzeigen, das mit der Schaltfläche **Liste** geöffnet wird.

Als zusätzliche Schutzoption wird empfohlen, die Zwischenspeicherung von Domänennamen bei der Arbeit mit Internetressourcen zu deaktivieren. Dieser Dienst verkürzt die Verbindungszeit Ihres Computers mit erforderlichen Internetressourcen wesentlich, stellt aber gleichzeitig eine gefährliche Schwachstelle dar, die von Angreifern benutzt werden kann, um einen Kanal für den Zugriff auf Ihre Daten zu organisieren, dessen Kontrolle mit einer Firewall nicht möglich ist. Deshalb wird zur Steigerung der Sicherheit Ihres Computers

empfohlen, das Speichern von Informationen über Domänennamen im Cache abzuschalten.

3.2.9. Abschluss des Konfigurationsassistenten

Im letzten Fenster des Assistenten wird Ihnen angeboten, den Computer neu zu starten, um die Programminstallation fertig zu stellen. Der Neustart ist notwendig, um die Treiber von Kaspersky Internet Security zu registrieren.

Sie können den Neustart des Computers aufschieben. Allerdings werden in diesem Fall bestimmte Schutzkomponenten der Anwendung nicht funktionieren.

3.3. Installation der Anwendung aus der Befehlszeile

Geben Sie zur Installation von Kaspersky Internet Security in der Befehlszeile ein:

```
msiexec /i <Paketname>
```

Der Installationsassistent (s. Pkt. 3.1 auf S. 34) wird gestartet. Zum Abschluss der Anwendungsinstallation ist der Neustart des Computers erforderlich.

Außerdem können Sie zur Installation der Anwendung eine der folgenden Methoden verwenden.

Um die Anwendung im Silent-Modus ohne Neustart des Computers zu installieren (der Neustart muss nach der Installation manuell erfolgen), geben Sie folgende Befehlszeile ein:

```
msiexec /i <Paketname> /qn
```

Um die Anwendung im Silent-Modus mit anschließendem Neustart des Computers zu installieren, geben Sie folgende Befehlszeile ein:

```
msiexec /i <Paketname> ALLOWREBOOT=1 /qn
```

3.4. Aktualisierung der Anwendung von Version 5.0 auf Version 6.0

Wenn auf Ihrem Computer die Anwendung Kaspersky Anti-Virus 5.0 for Windows Workstations, Kaspersky Anti-Virus Personal oder Kaspersky Anti-

Virus Personal Pro installiert ist, können Sie diese auf Kaspersky Internet Security 6.0 aktualisieren.

Nach dem Start des Installationsprogramms für Kaspersky Internet Security 6.0 wird Ihnen angeboten, zuerst die fünfte Version des Produkts zu entfernen. Nach Abschluss der Deinstallation ist der Neustart des Computers notwendig. Danach beginnt die Installation der Anwendung der Version 6.0.

Vorsicht!

Wenn Sie Kaspersky Internet Security 6.0 über die Vorgängerversion des Produkts installieren und die Installation aus einem Netzwerkordner erfolgt, auf den der Zugriff mit Hilfe eines Kennworts eingeschränkt ist, beachten Sie folgende Besonderheit. Nach dem Löschen der Anwendung der Version 5.0 und dem Neustart des Computers, erhält das Installationsprogramm keinen Zugriff auf den Netzwerkordner, in dem sich die Distribution der Anwendung befindet. Deshalb wird die Installation des Produkts abgebrochen. Um die korrekte Installation der Anwendung zu gewährleisten, starten Sie diese nur aus einer lokalen Ressource.

KAPITEL 4. PROGRAMM-OBERFLÄCHE

Kaspersky Internet Security verfügt über eine einfache und komfortable Oberfläche. In diesem Kapitel werden die wichtigsten Elemente der Oberfläche ausführlich beschrieben:

- Symbol im Infobereich der Taskleiste (s. Pkt. 4.1 auf S. 52)
- Kontextmenü (s. Pkt. 4.2 auf S. 53)
- Hauptfenster (s. Pkt. 4.3 auf S. 55)
- Konfigurationsfenster der Anwendung (s. Pkt. 4.4 auf S. 58)

Das Programm verfügt außer der Hauptoberfläche noch über Erweiterungskomponenten (PlugIns), die in folgende Anwendungen integriert werden können:

- Microsoft Outlook: Virenuntersuchung (s. Pkt. 8.2.2 auf S. 117) und Spam-Untersuchung (s. Pkt. 13.3.9 auf S. 213)
- Microsoft Outlook Express (s. Pkt. 13.3.10 auf S. 217)
- The Bat!: Virenuntersuchung (s. Pkt. 8.2.3 auf S. 118) und Spam-Untersuchung (s. Pkt. 13.3.11 auf S. 218)
- Microsoft Internet Explorer (s. Kapitel 11 auf S. 156)
- Microsoft Windows Explorer (s. Pkt. 14.2 auf S. 223)

Die PlugIns erweitern die Möglichkeiten der genannten Programme, da auf ihrer Oberfläche die Steuerung und Konfiguration der entsprechenden Komponenten von Kaspersky Internet Security möglich ist.

4.1. Symbol im Infobereich

Sofort nach der Installation von Kaspersky Internet Security erscheint sein Symbol im Infobereich der Taskleiste.

Das Symbol ist ein spezieller Indikator für die Arbeit von Kaspersky Internet Security. Er informiert über den Schutzstatus und eine Reihe wichtiger Aufgaben, die vom Programm ausgeführt werden.

Wenn das Symbol aktiv (farbig) ist, ist der Schutz Ihres Computers aktiviert. Ist das Symbol inaktiv (schwarz-weiß), dann ist der Schutz vollständig

deaktiviert oder bestimmte Schutzkomponenten wurden angehalten (s. Pkt. 2.2.1 auf S. 27).

Abhängig von der momentan ausgeführten Operation verändert sich das Symbol von Kaspersky Internet Security:



Die Untersuchung einer E-Mail-Nachricht wird ausgeführt.

Die Skriptuntersuchung wird ausgeführt.

Die Untersuchung einer Datei, die von Ihnen oder einem Programm geöffnet, gespeichert oder gestartet wird, wird ausgeführt.

Das Update der Bedrohungssignaturen und Programm-Module von Kaspersky Internet Security wird ausgeführt.

Bei der Arbeit einer Komponente von Kaspersky Internet Security ist eine Störung aufgetreten.

Das Symbol bietet außerdem Zugriff auf die grundlegenden Elemente der Programmoberfläche: Kontextmenü (s. Pkt. 4.2 auf S. 53) und Hauptfenster (s. Pkt. 4.3 auf S. 55).

Um das Kontextmenü zu öffnen, klicken Sie mit der rechten Maustaste auf das Programmsymbol.

Um das Hauptfenster von Kaspersky Internet Security im Abschnitt **Schutz** zu öffnen (mit diesem Abschnitt startet das Programm standardmäßig), doppelklicken Sie mit der linken Maustaste auf das Programmsymbol. Durch einfaches Klicken wird das Hauptfenster in dem Abschnitt geöffnet, der aktiv war, bevor es geschlossen wurde.

4.2. Kontextmenü

Das Kontextmenü (s. Abb. 1) bietet Zugriff auf die wichtigsten Schutzaufgaben.



Abbildung 1. Kontextmenü

Das Menü von Kaspersky Internet Security enthält folgende Punkte:

Arbeitsplatz untersuchen – Starten der vollständigen Untersuchung Ihres Computers auf das Vorhandensein von Viren. Dadurch werden die Objekte auf allen Laufwerken einschließlich der Wechseldatenträger untersucht.

Virensuche – Zur Auswahl von Objekten wechseln und die Virensuche in diesen Objekten starten. Standardmäßig enthält die Liste bestimmte Objekte wie beispielsweise den Ordner **Eigene Dateien**, Autostart-Objekte, Maildatenbanken, alle Laufwerke Ihres Computers usw. Sie können die Liste ergänzen, Objekte zur Untersuchung auswählen und die Virensuche starten.

Update – Die Updates der Programm-Module und Datenbanken für Kaspersky Internet Security herunterladen und auf Ihrem Computer installieren.

Netzwerkmonitor – Ansicht einer Liste der aktiven Netzwerkverbindungen, der offenen Ports und des Datenverkehrs.

Netzwerkverkehr blockieren – Alle Netzwerkverbindungen des Computers vorübergehend sperren. Durch Auswahl dieses Menüpunkts ändert sich die Sicherheitsstufe von Anti-Hacker (s. Pkt. 12.1 auf S. 168) in **Alle blockieren**. Um die Interaktion des Computers mit dem Netzwerk zu erlauben, wählen Sie erneut diesen Punkt im Kontextmenü.

Aktivierung – Zum Aktivieren des Programms wechseln. Dieser Menüpunkt ist nur vorhanden, wenn das Programm noch nicht aktiviert wurde.

Einstellungen – Zur Ansicht und Konfiguration der Funktionsparameter von Kaspersky Internet Security wechseln.

Kaspersky Internet Security – Das Programmhauptfenster öffnen (s. Pkt. 4.3 auf S. 55).

Schutz anhalten / **Schutz aktivieren** – Die Arbeit der Schutzkomponenten (s. Pkt. 2.2.1 auf S. 27) vorübergehend deaktivieren/aktivieren. Dieser

Menüpunkt hat keinen Einfluss auf das Programmupdate und die Ausführung der Aufgaben zur Virensuche.

Beenden – Die Arbeit von Kaspersky Internet Security beenden.

Wenn im Moment eine Aufgabe zur Virensuche läuft, wird ihr Name im Kontextmenü mit Prozentangabe des Ausführungsergebnisses angezeigt. Durch die Auswahl der Aufgabe gelangen Sie in das Berichtsfenster mit den aktuellen Ausführungsergebnissen.

4.3. Programmhauptfenster

Das Hauptfenster von Kaspersky Internet Security (s. Abb. 2) lässt sich bedingt in zwei Bereiche aufteilen:

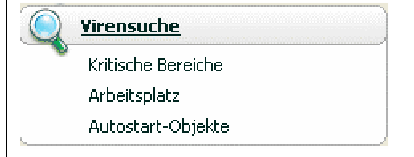
- Die linke Seite des Fensters, der *Navigationsbereich*, erlaubt es, schnell und einfach zu einer beliebigen Komponente, zur Ausführung der Aufgaben zur Virensuche oder zu den Servicefunktionen des Programms zu wechseln.
- Die rechte Seite des Fensters, der *Informationsbereich*, enthält Informationen über die auf der linken Seite ausgewählte Schutzkomponente, erlaubt den Wechsel zu den Einstellungen der einzelnen Komponenten, bietet Werkzeuge zur Ausführung der Aufgaben zur Virensuche, zur Arbeit mit Dateien in der Quarantäne und im Backup, zur Verwaltung der Lizenzschlüssel usw.



Abbildung 2. Hauptfenster von Kaspersky Internet Security

Wird auf der linken Seite des Fensters ein Abschnitt oder eine Komponente ausgewählt, dann erhalten Sie auf der rechten Seite vollständige Informationen darüber.

Hier werden die Elemente der Navigationsleiste des Hauptfensters genauer beschrieben.

Abschnitt des Navigationsteils im Hauptfenster	Funktion
Die Hauptaufgabe des Fensters ist es, Sie über den Schutzstatus Ihres Computers zu informieren. Dazu dient der Abschnitt **Schutz**.  	Wählen Sie im Navigationsbereich den Abschnitt **Schutz**, um allgemeine Informationen über die Arbeit von Kaspersky Internet Security zu erhalten, eine zusammenfassende Statistik über die Arbeit des Programms zu lesen oder sich zu vergewissern, ob alle Komponenten korrekt funktionieren. Um die Funktionsparameter einer konkreten Schutzkomponente zu überprüfen, wählen Sie im Abschnitt **Schutz** den Namen der Komponente aus, über die Sie Informationen benötigen.
Für die Untersuchung des Computers auf die Existenz schädlicher Objekte ist der spezielle Abschnitt **Virensuche** vorgesehen.  	Dieser Abschnitt enthält eine Liste von Objekten, die Sie auf Viren untersuchen können. Die Aufgaben, die nach Meinung der Kaspersky-Lab-Experten in erster Linie ausgeführt werden sollten, sind in diesem Abschnitt enthalten. Das sind die Aufgaben zur Virensuche in kritischen Bereichen, unter den Autostart-Objekten und die vollständige Untersuchung des Computers.
Der Abschnitt **Service** enthält zusätzliche Funktionen von Kaspersky Internet Security.  	Hier können Sie zum Update der Anwendung wechseln, die Berichte über die Arbeit einer beliebigen Komponente oder Aufgabe von Kaspersky Internet Security ansehen, zur Arbeit mit den Objekten in der Quarantäne und mit den Sicherungskopien, zu Informationen über den technischen Kundendienst, zum Erstellen einer Notfall-CD für die System-wiederherstellung oder in das Fenster zur Lizenzschlüsselverwaltung wechseln.

Abschnitt des Navigationsteils im Hauptfenster	Funktion
Dieser Bereich begleitet Ihre Arbeit mit dem Programm durch **Kommentare und Ratschläge**. Achtung Es wurden schädliche Objekte gefunden. Die sofortige Desinfektion wird empfohlen. Alle desinfizieren Details...	In diesem Abschnitt können Sie jederzeit Ratschläge darüber erhalten, wie die Schutzstufe des Computers erhöht werden kann. Hier befinden sich Kommentare über die laufende Arbeit der Anwendung und ihre Einstellungen. Mit Hilfe der Hyperlinks dieses Abschnitts können Sie direkt zu der Ausführung der im konkreten Fall empfohlenen Aktionen übergehen oder ausführliche Informationen darüber erhalten.

Jedes Element des Navigationsbereichs verfügt über ein spezielles Kontextmenü. Für die Schutzkomponenten und die Servicefunktionen enthält das Menü beispielsweise Punkte, die es erlauben, schnell zu deren Einstellungen, zur Steuerung oder zur Berichtsansicht zu gelangen. Für die Aufgaben zur Virensuche ist ein zusätzlicher Menüpunkt vorgesehen, der es erlaubt, auf Basis der ausgewählten Aufgabe eine neue Aufgabe zu erstellen.

Sie können das Aussehen des Programms anpassen, indem Sie grafische Elemente und Farbschemen erstellen und verwenden.

4.4. Konfigurationsfenster der Anwendung

Das Konfigurationsfenster von Kaspersky Internet Security kann vom Hauptfenster aus aufgerufen werden (s. Pkt. 4.3 auf S. 55). Klicken Sie dazu auf den Link Einstellungen im oberen Bereich des Hauptfensters.

Die Struktur des Konfigurationsfensters (s. Abb. 3) entspricht jener des Hauptfensters:

- Die linke Seite des Fensters bietet schnellen und bequemen Zugriff auf die Einstellungen jeder Programmkomponente und Untersuchungsaufgabe, sowie auf die Einstellungen für die Servicefunktionen des Programms.
- Die rechte Seite des Fensters enthält eine Liste der Parameter für die auf der linken Seite ausgewählte Komponente, Aufgabe usw.

Wird auf der linken Seite des Konfigurationsfensters ein bestimmter Abschnitt, eine Komponente oder eine Aufgabe ausgewählt, dann werden auf der rechten Fensterseite die entsprechenden Parameter angezeigt. Zur Detaileinstellung bestimmter Parameter können Sie die Konfigurationsfenster der zweiten oder dritten Ebene öffnen. Eine ausführliche Beschreibung der Anwendungsparameter finden Sie in den Abschnitten des vorliegenden Benutzerhandbuchs.

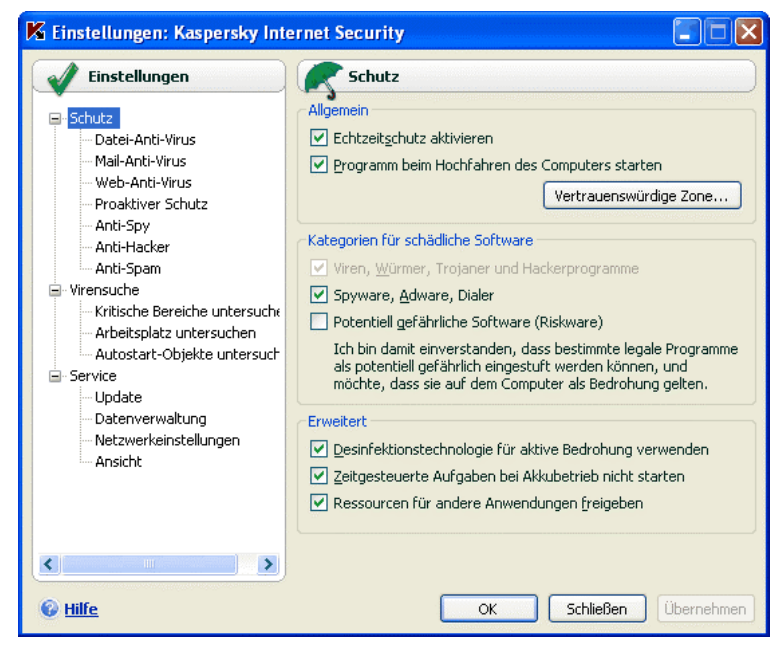


Abbildung 3. Konfigurationsfenster von Kaspersky Internet Security

KAPITEL 5. ERSTE SCHRITTE

Bei der Entwicklung von Kaspersky Internet Security bestand eine der Hauptaufgaben der Spezialisten von Kaspersky Lab in der optimalen Konfiguration aller Programmeinstellungen. Das verleiht einem Benutzer unabhängig von seiner Erfahrung mit Computern die Möglichkeit, sofort nach der Programminstallation die Sicherheit des Computers zu gewährleisten, ohne sich ausführlich mit den Einstellungen zu beschäftigen.

Allerdings können die Konfiguration Ihres Computers oder die auf diesem zu lösenden Aufgaben Besonderheiten aufweisen. Deshalb empfehlen wir Ihnen, das Programm zuerst anzupassen, um mit den Schutz mit maximaler Flexibilität genau auf Ihren Computer einzustellen.

Um die Benutzerfreundlichkeit zu erhöhen, haben wir uns bemüht, die Etappen der vorbereitenden Einstellungen in dem Konfigurationsassistenten (s. Pkt. 3.2 auf S. 39) zusammenzufassen, der am Ende der Programminstallation gestartet wird. Im Rahmen des Assistenten können Sie das Programm aktivieren, Einstellungen für das Update und den Start von Untersuchungsaufgaben vornehmen, den Zugriff auf das Programm mit Hilfe eines Kennworts beschränken und die Arbeit von Anti-Hacker auf Basis der Besonderheiten Ihres Netzwerks anpassen.

Wir empfehlen Ihnen, nach der Installation und dem Start des Programms auf Ihrem Computer folgende Aktionen vorzunehmen:

- Bewertung des aktuellen Schutzstatus, um sicherzustellen, dass Kaspersky Internet Security den Schutz auf der erforderlichen Stufe gewährleistet (s. Pkt. 5.1 auf S. 61).
- Training von Anti-Spam bei der Arbeit mit Ihren E-Mails (s. Pkt. 5.5 auf S. 69).
- Update des Programms, wenn das Update nicht mit Hilfe des Konfigurationsassistenten oder automatisch sofort nach der Programminstallation erfolgte (s. Pkt. 5.6 auf S. 70).
- Untersuchung des Computers auf das Vorhandensein von Viren (s. Pkt. 5.2 auf S. 66).

5.1. Welchen Schutzstatus hat mein Computer?

Zusammenfassende Informationen über den Schutz Ihres Computers befinden sich im Hauptfenster von Kaspersky Internet Security im Abschnitt **Schutz**. Hier werden der aktuelle *Schutzstatus* des Computers und die *Gesamtstatistik über die Arbeit* des Programms angezeigt.

Der **Schutzstatus** gibt den aktuellen Schutzstatus Ihres Computers mit Hilfe spezieller Indikatoren (s. Pkt. 5.1.1 auf S. 61) wieder. Die Statistik (s. Pkt. 5.1.2 auf S. 64) enthält die Ergebnisse der laufenden Programmarbeit.

5.1.1. Schutzindikatoren

Der **Schutzstatus** wird durch drei Indikatoren bestimmt, welche die Schutzstufe Ihres Computers zum aktuellen Zeitpunkt darstellen und auf Probleme in den Einstellungen und bei der Arbeit des Programms hinweisen.

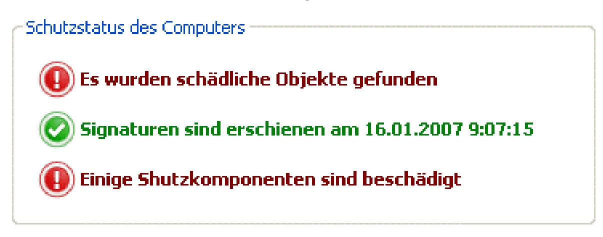
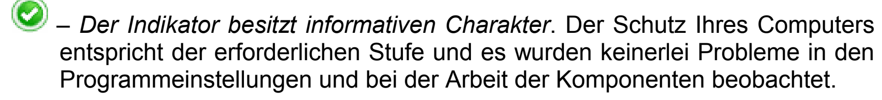


Abbildung 4. Indikatoren, die den Schutzstatus des Computers darstellen

Die Prioritätsstufe eines Ereignisses, das durch den Indikator dargestellt wird, kann einen der folgenden Werte besitzen:



– *Der Indikator besitzt informativen Charakter*. Der Schutz Ihres Computers entspricht der erforderlichen Stufe und es wurden keinerlei Probleme in den Programmeinstellungen und bei der Arbeit der Komponenten beobachtet.

– *Der Indikator warnt vor bestimmten Abweichungen* vom empfohlenen Funktionsmodus bei der Arbeit von Kaspersky Internet Security, die sich auf den Datenschutz auswirken können. Bitte beachten Sie unbedingt die Empfehlungen der Kaspersky-Lab-Spezialisten, die im Abschnitt für Kommentare und Tipps im Programmhauptfenster angezeigt werden.

– *Der Indikator verweist auf kritische Situationen* im Schutz Ihres Computers. Bitte befolgen Sie unbedingt die Empfehlungen der Kaspersky-Lab-

Spezialisten, die im Abschnitt für Kommentare und Tipps im Programmhauptfenster angezeigt werden. Sie dienen der Erhöhung des Schutzes Ihres Computers. Die empfohlenen Aktionen besitzen die Form von Links.

Im Folgenden werden die Schutzindikatoren und die ihnen entsprechenden Situationen genauer beschrieben.

Der erste Indikator weist auf eine Situation im Zusammenhang mit schädlichen Objekten auf Ihrem Computer hin. Der Indikator kann folgende Werte annehmen:



Es wurden keine schädlichen Objekte gefunden

Kaspersky Internet Security hat auf Ihrem Computer keinerlei gefährlichen Objekte gefunden.

Alle schädlichen Objekte wurden neutralisiert

Kaspersky Internet Security hat alle von Viren infizierten Objekte desinfiziert und irreparable Objekte gelöscht.



Es wurden schädliche Objekte gefunden

Auf Ihrem Computer besteht momentan das Risiko einer Infektion. Kaspersky Internet Security hat schädliche Objekte gefunden, deren Desinfektion erforderlich ist. Verwenden Sie dazu den Link Alle desinfizieren. Mit dem Link Details erhalten Sie Detailinformationen über die schädlichen Objekte.

Ein Hackerangriff wurde abgewehrt

Kaspersky Internet Security hat einen versuchten Netzwerkangriff erkannt und abgewehrt.

Der Neustart des Computers ist erforderlich

Um die schädlichen Objekte zu bearbeiten, ist der Neustart des Computers erforderlich. Speichern und schließen Sie alle Dateien, mit denen Sie gearbeitet haben, und verwenden Sie den Link Computer neu starten.

Der zweite Indikator gibt an, wie aktuell der Schutz Ihres Computers momentan ist. Der Indikator kann folgende Werte annehmen:



Signaturen sind erschienen am (Datum, Uhrzeit)

Das Programm benötigt keine Aktualisierung. Alle Dankenbanken, die bei der Arbeit von Kaspersky Internet Security verwendet werden, enthalten aktuelle Informationen für den Schutz Ihres Computers.



Signaturen sind nicht aktuell

Die Programm-Module und die Bedrohungssignaturen von Kaspersky Internet Security wurden seit mehreren Tagen nicht aktualisiert. Sie setzen Ihren Computer dem Risiko einer Infektion durch neue Schadprogramme oder neue Angriffe aus, die seit dem Tag des letzten Programmupdates aufgetaucht sind. Es wird nachdrücklich empfohlen, Kaspersky Internet Security zu aktualisieren. Verwenden Sie dazu den Link Aktualisieren.

Der Neustart des Computers ist erforderlich

Für die korrekte Aktualisierung des Programms ist der Systemneustart erforderlich. Speichern und schließen Sie alle Dateien, mit denen Sie gearbeitet haben, und verwenden Sie den Link Computer neu starten.

Signaturen sind veraltet

Kaspersky Internet Security wurde sehr lange nicht aktualisiert. Die Daten auf Ihrem Computer unterliegen einem großen Risiko. Aktualisieren Sie das Programm so schnell wie möglich. Verwenden Sie dazu den Link Aktualisieren.

Signaturen sind beschädigt/teilweise beschädigt

Die Dateien mit den Bedrohungssignaturen sind vollständig oder teilweise beschädigt. In diesem Fall wird empfohlen, das Programmupdate erneut zu starten. Wenn der Fehler durch das erneute Update nicht behoben werden kann, wenden Sie sich an den technischen Support-Service von Kaspersky Lab.

Der dritte Indikator gibt an, inwieweit die Möglichkeiten des Programms genutzt werden. Der Indikator kann folgende Werte annehmen:



Alle Schutzkomponenten sind aktiv

Kaspersky Internet Security schützt Ihren Computer auf allen Kanälen, über die schädliche Programme eindringen können. Alle Schutzkomponenten sind aktiviert.

Der Schutz ist nicht installiert

Bei der Installation von Kaspersky Internet Security wurde keine der Echtzeitschutz-Komponenten installiert. In diesem Fall steht nur die Virenuntersuchung von Objekten zur Verfügung. Um die maximale Sicherheit des Computers zu gewährleisten, wird empfohlen, die Schutzkomponenten zu installieren.



Einige Schutzkomponenten wurden angehalten

Die Arbeit einer oder mehrerer Schutzkomponenten wurde für einen bestimmten Zeitraum angehalten. Um die Arbeit der inaktiven Komponente wiederaufzunehmen, wählen Sie die Komponente in der Liste aus und klicken Sie auf die Schaltfläche ▶.

Alle Schutzkomponenten wurden angehalten

Die Arbeit aller Schutzkomponenten wurde für einen bestimmten Zeitraum angehalten. Um die Arbeit der Komponenten wiederaufzunehmen, wählen Sie im Kontextmenü den Punkt **Schutz aktivieren**. Das Kontextmenü wird durch Klick auf das Programmsymbol in der Taskleiste geöffnet.

Einige Schutzkomponenten wurden deaktiviert

Eine oder mehrere Schutzkomponenten sind abgeschaltet. Dies kann zu einer Infektion Ihres Computers und zu Datenverlust führen. Es wird ausdrücklich empfohlen, den Schutz zu aktivieren. Wählen Sie die inaktive Komponente in der Liste aus und klicken Sie auf die Schaltfläche ▶.

Alle Schutzkomponenten wurden deaktiviert

Der Schutz des Computers wurde vollständig abgeschaltet. Keine der Schutzkomponenten arbeitet. Um die Arbeit der Komponenten wiederaufzunehmen, wählen Sie im Kontextmenü den Punkt **Schutz aktivieren**. Das Kontextmenü wird durch Klick auf das Programmsymbol in der Taskleiste geöffnet.



Einige Schutzkomponenten sind beschädigt

Bei der Arbeit einer oder mehrerer Schutzkomponenten von Kaspersky Internet Security ist eine Störung eingetreten. In dieser Situation wird empfohlen, die Komponente zu aktivieren oder den Computer neu zu starten (möglicherweise ist nach der Übernahme von Updates die Registrierung von Komponententreibern erforderlich).

5.1.2. Status einer einzelnen Komponente von Kaspersky Internet Security

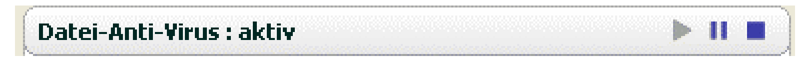
Um zu erfahren, wie Kaspersky Internet Security das Dateisystem, E-Mails, den HTTP-Datenstrom und andere Quellen schützt, über die gefährliche Programme auf Ihren Computer gelangen können, wie die Aufgaben zur Virensuche arbeiten

und wie das Update der Bedrohungssignaturen ausgeführt wird, öffnen Sie einfach den entsprechenden Abschnitt des Programmhauptfensters.

Um beispielsweise den aktuellen Status des Dateischutzes zu überprüfen, wählen Sie den Abschnitt **Datei-Anti-Virus** auf der linken Seite des Programmhauptfensters. Um sich über den Status des Schutzes vor Infektionen durch neue Viren zu informieren, öffnen Sie den Abschnitt **Proaktiver Schutz**. Auf der rechten Seite werden zusammenfassende Informationen über die Arbeit der Komponente angezeigt.

Für die Schutzkomponenten bestehen diese Informationen aus folgenden Elementen: **Statuszeile**, **Status** (für Untersuchungs- und Updateaufgaben – **Einstellungen**) und **Statistik**.

Betrachten wir als Beispiel die **Statuszeile** der Komponente Datei-Anti-Virus:



- *Datei-Anti-Virus* : aktiv – Der Dateischutz funktioniert auf der gewählten Stufe (s. Pkt. 7.1 auf S. 97).

- *Datei-Anti-Virus : Pause* – Der *Datei-Anti-Virus* wurde für einen bestimmten Zeitraum angehalten. Die Komponente nimmt ihre Arbeit automatisch nach Ablauf des festgelegten Zeitraums oder nach dem Neustart des Programms wieder auf. Sie können den Dateischutz manuell aktivieren. Klicken Sie dazu in der Statuszeile auf die Schaltfläche ▶.

- *Datei-Anti-Virus : deaktiviert* – Die Arbeit der Komponente wurde vom Benutzer beendet. Sie können den Dateischutz aktivieren. Klicken Sie dazu in der Statuszeile auf die Schaltfläche ▶.

- *Datei-Anti-Virus : funktioniert nicht* – Der Dateischutz ist aus bestimmten Gründen nicht verfügbar (beispielsweise wenn Sie keinen Lizenzschlüssel für die Nutzung des Programms besitzen).

- *Datei-Anti-Virus : Störung*– Die Komponente hat ihre Arbeit fehlerhaft abgeschlossen. Wenden Sie sich in diesem Fall an den technischen Support-Service von Kaspersky Lab.

Wenn die Komponente aus mehreren Modulen besteht, enthält der Abschnitt **Status** Informationen darüber, ob die einzelnen Module aktiviert oder deaktiviert sind. Für jene Komponenten, die nicht aus separaten Modulen bestehen, werden der Status der Komponente, die von ihr gewährleistete Sicherheitsstufe und für bestimmte Komponenten die Aktion für ein gefährliches Programm angezeigt.

Für Aufgaben zur Virensuche und zum Programmupdate ist der Block **Status** nicht vorhanden. Die Sicherheitsstufe, die im Rahmen der Virensuche auf ein gefährliches Programm anzuwendende Aktion und der Update-Startmodus werden im Block **Einstellungen** genannt.

Der Block **Statistik** enthält die Arbeitsergebnisse der Schutzkomponente, des Updates oder der Untersuchungsaufgabe.

5.1.3. Statistik der Programmarbeit

Die Statistik über die Arbeit des Programms wird im Block **Statistik** des Abschnitts **Schutz** im Programmhauptfenster angezeigt (s. Abb. 5) und enthält Informationen über den Schutz des Computers, die seit der Installation von Kaspersky Internet Security aufgezeichnet wurden.

Statistik

Insgesamt untersucht:	5222
Gefährliche Objekte gefunden:	9
Nicht desinfizierte Objekte:	1
Abgewehrte Angriffe:	0

Abbildung 5. Block mit Gesamtstatistik über die Arbeit des Programms

Durch Linksklick an eine beliebige Stelle des Blocks können Sie einen Bericht mit detaillierten Informationen öffnen. Auf den entsprechenden Registerkarten befinden sich folgende Informationen:

- Informationen über gefundene Objekte (s. Pkt. 17.3.2 auf S. 269) und den Status, der den Objekten zugewiesen wurde.
- Ereignisbericht (s. Pkt. 17.3.3 auf S. 270)
- Zusammenfassende Statistik über die Untersuchung des Computers (s. Pkt. 17.3.4 auf S. 271)
- Einstellungen für die Arbeit des Programms (s. Pkt. 17.3.5 auf S. 272)

5.2. Wie der Computer auf Viren untersucht wird

Nach der Installation der Anwendung werden Sie durch eine obligatorische Meldung im unteren linken Bereich des Anwendungsfensters darauf hingewiesen, dass noch keine Untersuchung des Computers ausgeführt wurde, und Ihnen wird empfohlen, ihn umgehend auf Viren zu untersuchen.

Der Lieferumfang von Kaspersky Internet Security umfasst eine Aufgabe zur Virensuche auf dem Computer. Diese befindet sich im Abschnitt **Virensuche** des Programmhauptfensters.

Nach der Auswahl der Aufgabe **Arbeitsplatz** können Sie auf der rechten Seite des Fensters eine Statistik der letzten Untersuchung des Computers und die Aufgabenparameter überprüfen: welche Schutzstufe wurde gewählt, welche Aktion wird auf gefährliche Objekte angewandt.

Um den Computer auf die Existenz von schädlichen Objekten zu untersuchen,

klicken Sie auf der rechten Seite des Fensters auf die Schaltfläche **Virensuche**.

Dadurch wird die Untersuchung Ihres Computers gestartet. Details der Untersuchung werden in einem speziellen Fenster angezeigt. Durch Klick auf die Schaltfläche **Schließen** wird das Fenster mit Informationen über den Untersuchungsvorgang ausgeblendet. Die Untersuchung wird dadurch nicht beendet.

5.3. Wie kritische Computerbereiche untersucht werden

Auf Ihrem Computer gibt es Bereiche, die hinsichtlich der Sicherheit als kritisch gelten. Sie können zum Objekt einer Infektion durch schädliche Programme werden, die auf die Beschädigung des Computerbetriebssystems, Prozessors, Arbeitsspeichers usw. gerichtet ist.

Es ist äußerst wichtig, die kritischen Bereiche des Computers zu schützen, um seine Funktionsfähigkeit aufrechtzuerhalten. Kaspersky Internet Security bietet eine spezielle Aufgabe zur Virensuche in diesen Bereichen. Sie befindet sich im Abschnitt **Virensuche** des Programmhauptfensters.

Nach der Auswahl der Aufgabe **Kritische Bereiche** können Sie auf der rechten Seite des Fensters eine Statistik der letzten Untersuchung dieser Bereiche und die Aufgabenparameter überprüfen: welche Schutzstufe wurde gewählt, welche Aktion wird auf gefährliche Objekte angewandt. Hier kann auch festgelegt werden, welche kritischen Bereiche untersucht werden sollen. Außerdem kann hier die Virensuche in den ausgewählten Bereichen gestartet werden.

Um die kritischen Computerbereiche auf die Existenz von schädlichen Objekten zu untersuchen,

klicken Sie auf der rechten Seite des Fensters auf die Schaltfläche **Virensuche**.

Dadurch wird die Untersuchung der ausgewählten Bereiche gestartet. Details der Untersuchung werden in einem speziellen Fenster angezeigt. Durch Klick auf die Schaltfläche **Schließen** wird das Fenster mit Informationen über den

Untersuchungsvorgang ausgeblendet. Die Untersuchung wird dadurch nicht beendet.

5.4. Wie eine Datei, ein Ordner oder ein Laufwerk auf Viren untersucht werden

In bestimmten Situationen ist es erforderlich, nicht den gesamten Computer, sondern nur ein einzelnes Objekt zu prüfen, beispielsweise eine Festplatte, auf der sich Programme und Spiele befinden, Maildatenbanken, die aus dem Büro mitgebracht wurden, ein Archiv, das per E-Mail empfangen wurde, usw. Sie können ein Objekt mit den Standardmitteln von Microsoft Windows auswählen (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.).

Um die Untersuchung des Objekts zu starten,

> führen Sie den Mauscursor auf den Namen des gewählten Objekts, öffnen durch Rechtsklick das Microsoft Windows-Kontextmenü und wählen den Punkt **Auf Viren untersuchen** (s. Abb. 6).

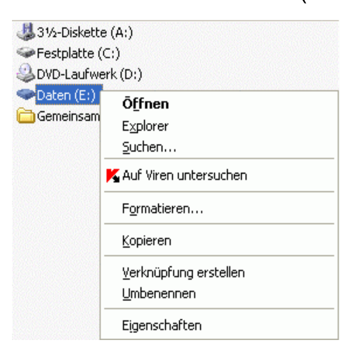


Abbildung 6. Virenuntersuchung eines Objekts, das über Microsoft Windows ausgewählt wurde

Dadurch wird die Untersuchung des ausgewählten Objekts gestartet. Details der Untersuchung werden in einem speziellen Fenster angezeigt. Durch Klick auf die Schaltfläche **Schließen** wird das Fenster mit Informationen über den Untersuchungsvorgang ausgeblendet. Die Untersuchung wird dadurch nicht beendet.

5.5. Wie Anti-Spam trainiert wird

Ein Schritt der Arbeitsvorbereitungen besteht darin, Anti-Spam für die Arbeit mit Ihren E-Mails zu trainieren. Spam ist unerwünschte Korrespondenz. Allerdings ist es schwierig, genau zu bestimmen, was für den einzelnen Benutzer als Spam gilt. Natürlich existieren Kategorien von Briefen, die sich mit hoher Wahrscheinlichkeit als Spam identifizieren lassen (beispielsweise massenhaft verschickte E-Mails, Werbung). Trotzdem können auch solche Briefe für bestimmte Anwender von Nutzen sein.

Deshalb bieten wir Ihnen an, selbständig festzulegen, welche E-Mails als Spam gelten und welche nicht. Kaspersky Internet Security schlägt Ihnen nach der Installation vor, die Komponente Anti-Spam zu trainieren, damit diese zwischen Spam und nützlicher Post unterscheiden kann. Dies kann entweder mit Hilfe spezieller Schaltflächen erfolgen, die in das Mailprogramm (Microsoft Office Outlook, Microsoft Outlook Express, The Bat!) integriert sind, oder mit Hilfe eines speziellen Trainingsassistenten.

Achtung!

In dieser Version von Kaspersky Internet Security sind keine Anti-Spam-Erweiterungsmodule für die 64-Bit-Versionen der Mailprogramme Microsoft Office Outlook, Microsoft Outlook Express und The Bat! vorgesehen.

Um Anti-Spam mit Hilfe spezieller Schaltflächen zu trainieren,

1. Öffnen Sie das Mailprogramm, das standardmäßig auf Ihrem Computer verwendet wird, beispielsweise Microsoft Office Outlook. Auf der Symbolleiste befinden sich zwei Schaltflächen: **Spam** und **Kein Spam**.
2. Wählen Sie einen nützlichen Brief oder eine Briefgruppe, die nützliche Briefe enthält, und klicken Sie auf die Schaltfläche **Kein Spam**. E-Mail-Nachrichten von den Absendern, deren Briefe Sie ausgewählt haben, gelten künftig als erwünschte Post.
3. Wählen Sie einen Brief, der für Sie nutzlose Informationen enthält, eine Gruppe von Briefen oder einen Ordner mit solchen Briefen, und klicken Sie auf die Schaltfläche **Spam**. Anti-Spam analysiert den Inhalt dieser Nachrichten und künftig werden alle Briefe ähnlichen Inhalts mit hoher Wahrscheinlichkeit als Spam bewertet.

Um Anti-Spam mit Hilfe des speziellen Assistenten zu trainieren,

1. Wählen Sie die Komponente Anti-Spam im Abschnitt **Schutz** des Programmhauptfensters und klicken Sie auf den Link **Einstellungen**.
2. Klicken Sie auf der rechten Seite des Konfigurationsfensters auf die Schaltfläche **Trainingsassistent**.

3. Wählen Sie beim ersten Schritt die Ordner Ihres Mailprogramms, die nützliche Post enthalten. Klicken Sie auf **Weiter**.

4. Geben Sie beim zweiten Schritt die Ordner mit unerwünschter Post an. Klicken Sie auf **Weiter**.

Das Training wird aufgrund der von Ihnen angegebenen Ordner ausgeführt.

Wenn eine E-Mail in Ihrer Mailbox eintrifft, untersucht Anti-Spam sie auf Spam und fügt einer unerwünschten Nachricht in der Kopfzeile **Betreff** die Markierung [Spam] hinzu. Sie können im Mailprogramm eine spezielle Regel für solche Briefe erstellen, beispielsweise eine Regel zum Löschen oder zum Verschieben in einen speziellen Ordner.

5.6. Wie das Programm aktualisiert wird

Kaspersky Lab aktualisiert die Bedrohungssignaturen und die Programm-Module von Kaspersky Internet Security und verwendet dazu spezielle Updateserver.

Kaspersky-Lab-Updateserver sind Internetseiten von Kaspersky Lab, auf denen Programmupdates zur Verfügung stehen.

> Achtung!
>
> Für das Update von Kaspersky Internet Security ist eine bestehende Internetverbindung erforderlich.

Kaspersky Internet Security überprüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Servern neue Updates vorhanden sind. Wenn auf dem Server neue Updates angeboten werden, lädt Kaspersky Internet Security sie im Hintergrundmodus herunter und installiert sie.

Um Kaspersky Internet Security manuell zu aktualisieren,

wählen Sie die Komponente **Update** im Abschnitt **Service** des Programmhauptfensters und klicken Sie auf der rechten Seite auf die Schaltfläche **Update**.

Dadurch wird die Aktualisierung von Kaspersky Internet Security gestartet. Alle Details über den Prozess werden in einem speziellen Fenster angezeigt.

5.7. Was tun, wenn der Schutz nicht funktioniert?

Sollten bei der Arbeit einer beliebigen Schutzkomponente Probleme oder Fehler auftreten, beachten Sie unbedingt ihren Status. Wenn als Status der Komponente *funktioniert nicht* oder *Störung* angezeigt wird, versuchen Sie, Kaspersky Internet Security neu zu starten.

Sollte das Problem nach dem Neustart der Anwendung weiter bestehen, wird empfohlen, mögliche Fehler mit Hilfe des Reparaturprogramms für die Anwendung zu korrigieren (**Start→Programme→Kaspersky Internet Security 6.0 →Ändern, Reparieren oder Löschen**).

Falls der Reparaturversuch erfolglos sein sollte, wenden Sie sich an den technischen Support-Service von Kaspersky Lab. Es kann erforderlich sein, den Bericht über die Arbeit der Komponente oder der gesamten Anwendung in einer Datei zu speichern und ihn zur Analyse an den Support-Service zu schicken.

Um den Bericht in einer Datei zu speichern,

1. Wählen Sie die Komponente im Abschnitt **Schutz** des Programmhauptfensters und klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Statistik**.
2. Klicken Sie auf die Schaltfläche **Speichern unter** und geben Sie im folgenden Fenster den Namen der Datei an, in welcher die Arbeitsergebnisse der Komponente gespeichert werden sollen.

Um einen Bericht aller Komponenten von Kaspersky Internet Security zu speichern (Komponenten für den Schutz, die Aufgaben zur Virensuche und die Servicefunktionen),

1. Wählen Sie den Abschnitt **Schutz** im Programmhauptfenster und klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Statistik**.

   oder

   Verwenden Sie im Berichtsfenster einer beliebigen Komponente den Hyperlink Liste aller Berichte. Dadurch werden die Berichte aller Programmkomponenten auf der Registerkarte **Berichte** angezeigt.
2. Klicken Sie auf die Schaltfläche **Speichern unter** und geben Sie im folgenden Fenster den Namen der Datei an, in welcher die Arbeitsergebnisse des Programms gespeichert werden sollen.

KAPITEL 6. KOMPLEXE STEUERUNG DES SCHUTZES

Kaspersky Internet Security bietet Ihnen die Möglichkeit zur komplexen Steuerung seiner Arbeit:

- Aktivieren, Deaktivieren oder Anhalten der Arbeit des Programms (s. Pkt. 6.1 auf S. 72).
- Die Typen gefährlicher Programme festlegen, vor denen Kaspersky Internet Security Ihren Computer schützen soll (s. Pkt. 6.2 auf S. 77).
- Erstellen einer Liste von Ausnahmen für den Schutz (s. Pkt. 6.3 auf S. 79).
- Erstellen eigener Aufgaben für die Virensuche und das Update (s. Pkt. 6.4 auf S. 89).
- Festlegen eines eigenen Zeitplans für den Aufgabenstart (s. Pkt. 6.5 auf S. 91).
- Anpassen der Leistungsparameter (s. Pkt. 6.6 auf S. 93) für den Computerschutz.

6.1. Computerschutz deaktivieren/ aktivieren

Kaspersky Internet Security wird standardmäßig beim Start des Betriebssystems gestartet, worüber Sie durch den Hinweis *Kaspersky Internet Security 6.0* rechts oben auf dem Bildschirm informiert werden, und schützt Ihren Computer während der gesamten Sitzung. Alle Schutzkomponenten sind aktiv (s. Pkt. 2.2.1 auf S. 27).

Sie können den von Kaspersky Internet Security gewährleisteten Schutz vollständig oder teilweise deaktivieren.

Achtung!

Die Kaspersky-Lab-Spezialisten **warnen ausdrücklich davor, den Schutz zu deaktivieren**, weil dies zur Infektion Ihres Computers und zu Datenverlust führen kann.

Beachten Sie, dass der Schutz hier ausdrücklich im Kontext der Schutzkomponenten beschrieben wird. Das Deaktivieren oder das Anhalten der Arbeit von Schutzkomponenten übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und auf das Programmupdate aus.

6.1.1. Schutz anhalten

Das Anhalten des Schutzes bedeutet, dass alle seine Komponenten, welche die Dateien auf Ihrem Computer, eingehende und ausgehende Post, auszuführende Skripts und das Verhalten der Anwendungen kontrollieren, sowie Anti-Hacker und Anti-Spam für einen bestimmten Zeitraum deaktiviert werden.

Um die Arbeit von Kaspersky Internet Security anzuhalten,

1. Wählen Sie im Kontextmenü (s. Pkt. 4.2 auf S. 53) des Programms den Punkt **Schutz anhalten**.
2. Wählen Sie im folgenden Fenster zum Deaktivieren des Schutzes (s. Abb. 7) den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:
   - **In <Zeitraum>** – Der Schutz wird nach Ablauf des festgelegten Zeitraums wieder aktiviert. Verwenden Sie die Dropdown-Liste, um den Wert für das Zeitintervall festzulegen.
   - **Nach dem Neustart des Programms** – Der Schutz wird aktiviert, wenn Sie das Programm aus dem Menü **Start** starten oder nachdem das System neu gestartet wurde (unter der Bedingung, dass der Modus für den Programmstart beim Hochfahren des Computers aktiviert ist (s. Pkt. 6.1.5 auf S. 77).
   - **Nur auf Befehl des Benutzers** – Der Schutz wird erst dann wieder aktiviert, wenn Sie ihn starten. Wählen Sie den Punkt **Schutz aktivieren** im Kontextmenü des Programms, um den Schutz zu aktivieren.

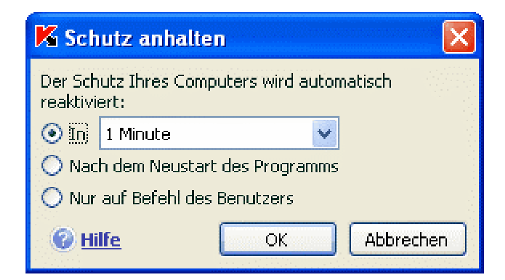


Abbildung 7. Fenster zum Anhalten des Computerschutzes

> Hinweis:
>
> Um den Schutz Ihres Computers zu deaktivieren, können Sie auch eine der folgenden Methoden verwenden:
>
> - Klicken Sie auf die Schaltfläche ❚❚ im Abschnitt **Schutz**.
> - Wählen Sie im Kontextmenü den Punkt **Beenden**. In diesem Fall wird das Programm beendet.

Durch das vorübergehende Deaktivieren wird die Arbeit aller Schutzkomponenten angehalten. Darüber informieren:

- Die inaktiven (graue Farbe) Namen der deaktivierten Komponenten im Abschnitt **Schutz** des Hauptfensters.
- Das inaktive (graue) Programmsymbol im Infobereich der Taskleiste.
- Der dritte Schutzindikator (s. Pkt. 5.1.1 auf S. 61) Ihres Computers zeigt folgenden Hinweis: **Alle Schutzkomponenten wurden angehalten**.

6.1.2. Computerschutz vollständig deaktivieren

Das vollständige Deaktivieren des Schutzes bedeutet, dass die Arbeit der Schutzkomponenten beendet wird. Die Virensuche und das Update funktionieren weiterhin im vorgegebenen Modus.

Wenn der Schutz vollständig deaktiviert wurde, kann er nur auf Befehl des Benutzers wieder aktiviert werden. In diesem Fall erfolgt kein automatisches Aktivieren der Schutzkomponenten nach dem Neustart des Systems oder des Programms. Beachten Sie, dass bei Konflikten zwischen Kaspersky Internet Security und anderen auf Ihrem Computer installierten Programmen die Arbeit

einer einzelnen Schutzkomponente angehalten oder eine Liste von Ausnahmen angelegt werden kann (s. Pkt. 6.3 auf S. 79).

Um den Computerschutz vollständig zu deaktivieren,

1. Öffnen Sie das Hauptfenster von Kaspersky Internet Security.
2. Wählen Sie den Abschnitt **Schutz** und klicken Sie auf den Link Einstellungen.
3. Deaktivieren Sie im Konfigurationsfenster des Programms das Kontrollkästchen **Schutz aktivieren**.

Durch das Deaktivieren des Schutzes wird die Arbeit aller seiner Komponenten beendet. Darüber informieren:

- Die inaktiven (grauen) Namen der deaktivierten Komponenten im Abschnitt **Schutz** des Hauptfensters.
- Das inaktive (graue) Programmsymbol im Infobereich der Taskleiste.
- Der dritte Schutzindikator (s. Pkt. 5.1.1 auf S. 61) Ihres Computers, zeigt folgenden Hinweis: **Alle Schutzkomponenten wurden deaktiviert**.

6.1.3. Schutzkomponente, Untersuchungs- oder Updateaufgabe anhalten/ beenden

Es gibt mehrere Methoden, um die Arbeit einer Schutzkomponente, einer Aufgabe zur Virensuche oder zum Update zu deaktivieren. Vor dem Deaktivieren sollten Sie allerdings Ihre Gründe dafür genau abwägen. Höchstwahrscheinlich besteht eine andere Möglichkeit, beispielsweise die Wahl einer anderen Sicherheitsstufe. Wenn Sie beispielsweise mit einer bestimmten Datenbank arbeiten, von der Sie sicher sind, dass sie virusfrei ist, geben Sie das Verzeichnis mit ihren Dateien einfach als Ausnahme an (s. Pkt. 6.3 auf S. 79).

Um die Arbeit einer Schutzkomponente bzw. die Ausführung einer Untersuchungs- oder Updateaufgabe anzuhalten,

wählen Sie die Komponente oder die Aufgabe im entsprechenden Abschnitt auf der linken Seite des Hauptfensters aus und klicken Sie in der Statuszeile auf die Schaltfläche .

Der Status der Komponente (Aufgabe) ändert sich in *Pause*. Der durch die Komponente gewährleistete Schutz bzw. die ausgeführte Aufgabe wird angehalten, bis Sie ihre Arbeit mit Hilfe der Schaltfläche neu starten.

Wenn Sie die Arbeit einer Komponente oder einer Aufgabe anhalten, wird die Statistik in der laufenden Sitzung von Kaspersky Internet Security gespeichert. Die Statistik wird fortgeführt, wenn die Arbeit der Komponente oder Aufgabe wieder aufgenommen wird.

Um die Arbeit einer Schutzkomponente, die Virensuche oder das Update zu beenden,

klicken Sie in der Statuszeile auf die Schaltfläche ■. Die Arbeit von Schutzkomponenten kann auch im Konfigurationsfenster des Programms beendet werden, indem das Kontrollkästchen ☑ **<Komponentenname> aktivieren** im Block **Allgemein** deaktiviert wird.

In diesem Fall ändert sich der Status der Komponente (Aufgabe) in *deaktiviert* (*abgebrochen*). Der durch die Komponente gewährleistete Schutz oder die ausgeführte Aufgabe wird beendet, bis Sie ihn/sie mit Hilfe der Schaltfläche ▶ neu starten. Für eine Untersuchungs- und Updateaufgabe werden Ihnen folgende Aktionen zur Auswahl angeboten: Ausführung der abgebrochenen Aufgabe fortsetzen oder Aufgabe neu starten.

Beim Beenden einer Schutzkomponente oder einer Aufgabe wird die gesamte Statistik über die bisherige Arbeit zurückgesetzt und beim Start der Komponente neu erstellt.

6.1.4. Computerschutz wiederherstellen

Wenn Sie zu einem gewissen Zeitpunkt den Schutz Ihres Computers angehalten oder vollständig deaktiviert haben, dann kann er durch eine der folgenden Methoden wieder aktiviert werden:

- *Aus dem Kontextmenü*.

  Wählen Sie dazu den Punkt **Schutz aktivieren**.

- *Aus dem Programmhauptfenster*.

  Klicken Sie dazu auf die Schaltfläche ▶ in der Statuszeile des Abschnitts **Schutz** des Hauptfensters.

Der Schutzstatus ändert sich sofort in *aktiv*. Das Programmsymbol im Infobereich wird aktiv (farbig). Der dritte Schutzindikator (s. Pkt. 5.1.1 auf S. 61) des Computers, zeigt folgenden Hinweis: ✅ **Alle Schutzkomponenten sind aktiv**.

6.1.5. Arbeit mit der Anwendung beenden

Wenn es aus einem bestimmten Grund erforderlich ist, die Arbeit von Kaspersky Internet Security vollständig zu beenden, wählen Sie den Punkt **Beenden** im Kontextmenü (s. Pkt. 4.2 auf S. 53) des Programms. Dadurch wird das Programm aus dem Arbeitsspeicher entfernt, was bedeutet, dass Ihr Computer dann ungeschützt ist.

Wenn im Augenblick, als die Arbeit des Programms beendet wurde, auf dem Computer Netzwerkverbindungen vorhanden waren, die vom Programm kontrolliert wurden, dann erscheint auf dem Bildschirm eine Meldung darüber, dass diese Verbindungen getrennt wurden. Das ist eine Voraussetzung für das korrekte Beenden des Programms. Die Verbindungen werden automatisch nach 10 Sekunden oder durch Klick auf die Schaltfläche **Ja** getrennt. Die Mehrzahl der getrennten Verbindungen wird nach einem bestimmten Zeitraum wiederhergestellt.

Hinweis: Wenn Sie während der Verbindungstrennung eine Datei herunterladen und dabei keinen Download-Manager verwenden, wird die Datenübertragung abgebrochen. Um die Datei herunterzuladen, müssen Sie den Download erneut initiieren.

Sie können das Trennen der Verbindungen ablehnen. Klicken Sie dazu im Meldungsfenster auf die Schaltfläche **Nein**. Dabei setzt das Programm seine Arbeit fort.

Nachdem Sie die Arbeit des Programms beendet haben, kann der Schutz des Computers erneut aktiviert werden, indem das Programm Kaspersky Internet Security über das Menü **Start** → **Programme** → **Kaspersky Internet Security 6.0** → **Kaspersky Internet Security 6.0** gestartet wird.

Außerdem kann der Schutz nach dem Neustart des Betriebssystems automatisch gestartet werden. Um diesen Modus zu wählen, verwenden Sie im Konfigurationsfenster des Programms den Abschnitt **Schutz** und aktivieren Sie das Kontrollkästchen ☑ **Programm beim Hochfahren des Computers starten**.

6.2. Typen der zu kontrollierenden schädlichen Programme

Kaspersky Internet Security bietet Ihnen Schutz vor verschiedenen Arten schädlicher Programme. Viren, trojanische Programme und Hacker-Utilities werden unabhängig von den Einstellungen von der Anwendung stets untersucht und neutralisiert. Diese Programme können Ihrem Computer ernsten Schaden

zufügen. Um die Sicherheit des Computers zu erhöhen, können Sie die Liste der erkennbaren Bedrohungen erweitern. Aktivieren Sie dazu die Kontrolle über unterschiedliche Arten potentiell gefährlicher Programme.

Um auszuwählen, vor welchen Arten schädlicher Programme Kaspersky Internet Security den Computer schützen soll, wählen Sie im Konfigurationsfenster des Programms (s. Pkt. 4.4 auf S. 58) den Abschnitt **Schutz**.

Die Bedrohungstypen (s. Pkt. 1.1 auf S. 11) werden im Block **Kategorien für schädliche Software** genannt:

- **Viren, Würmer, Trojaner und Hackerprogramme**. Diese Gruppe umfasst die meistverbreiteten und gefährlichsten Kategorien schädlicher Programme. Der Schutz vor diesen Bedrohungen gewährleistet das minimal erforderliche Sicherheitsniveau. In Übereinstimmung mit den Empfehlungen der Kaspersky-Lab-Spezialisten kontrolliert Kaspersky Internet Security die schädlichen Programme dieser Kategorie immer.
- **Spyware, Adware, Dialer**. Diese Gruppe enthält potentiell gefährliche Software, die den Benutzer behindern oder dem Computer bedeutenden Schaden zufügen kann.
- **Potentiell gefährliche Software (Riskware)**. Diese Gruppe umfasst Programme, die nicht schädlich oder gefährlich sind, aber unter bestimmten Umständen benutzt werden können, um Ihrem Computer Schaden zuzufügen.

Die genannten Gruppen bestimmen die Größe der Bedrohungssignaturen, die bei der Objektuntersuchung im Echtzeitschutz und bei der Virensuche auf Ihrem Computer verwendet werden.

Wenn alle Gruppen gewählt wurden, bietet Kaspersky Internet Security den maximalen Virenschutz Ihres Computers. Wenn die zweite und dritte Gruppe deaktiviert ist, schützt das Programm Sie nur vor den meistverbreiteten schädlichen Objekten. Dabei werden potentiell gefährliche und andere Programme nicht kontrolliert, die auf Ihrem Computer installiert werden können und durch ihre Aktionen Imageverlust und materiellen Schaden verursachen können.

Die Kaspersky-Lab-Spezialisten warnen davor, die Kontrolle der zweiten Gruppe zu deaktivieren. Sollte es vorkommen, dass Kaspersky Internet Security ein Programm als gefährlich klassifiziert, das Ihrer Meinung nach kein Risiko darstellt, wird empfohlen, es als Ausnahme festzulegen (s. Pkt. 6.3 auf S. 79).

6.3. Aufbau einer vertrauenswürdigen Zone

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste von Objekten, die das Programm Kaspersky Internet Security bei seiner Arbeit nicht kontrolliert. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz des Programms.

Die vertrauenswürdige Zone wird vom Benutzer unter Berücksichtigung der Besonderheiten von Objekten, mit denen er arbeitet, sowie von Programmen, die auf seinem Computer installiert sind, aufgebaut. Das Anlegen einer solchen Liste mit Ausnahmen kann beispielsweise erforderlich sein, wenn Kaspersky Internet Security den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt bzw. Programm absolut unschädlich ist.

Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm), Programmprozesse oder Objekte entsprechend der Klassifikation der Viren-Enzyklopädie (nach dem Status, der dem Objekt bei der Untersuchung von der Anwendung zugewiesen wurde) ausgeschlossen werden.

> Achtung!
>
> Ein ausgeschlossenes Objekt unterliegt nicht der Untersuchung, wenn das Laufwerk oder der Ordner untersucht wird, auf dem es sich befindet. Wird allerdings ein konkretes Objekt zur Untersuchung ausgewählt, dann wird die Ausnahmeregel ignoriert.

Um eine Liste von Ausnahmen für den Schutz zu erstellen,

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security und wählen Sie den Abschnitt **Schutz**.
2. Klicken Sie auf die Schaltfläche **Vertrauenswürdige Zone** im Block **Allgemein**.
3. Konfigurieren Sie im folgenden Fenster (s. Abb. 8) die Ausnahmeregeln für Objekte und legen Sie die Liste der vertrauenswürdigen Anwendungen an.

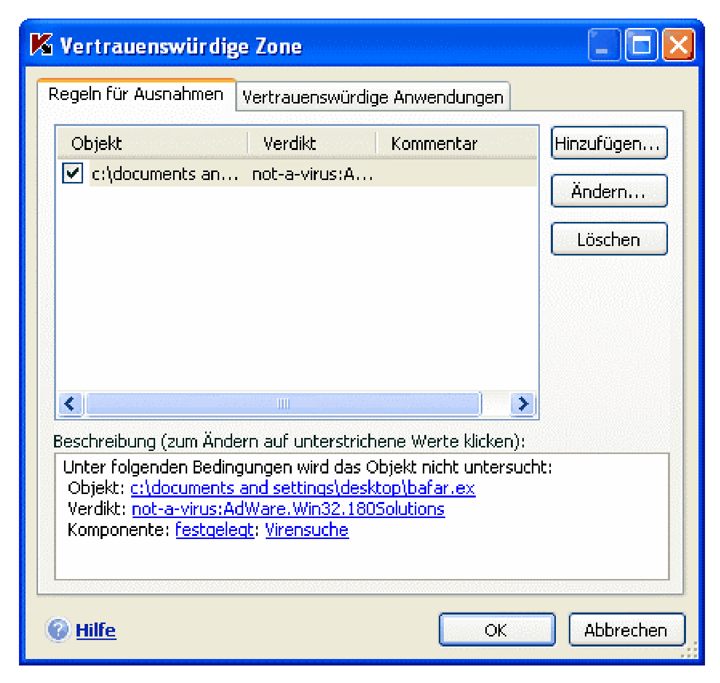


Abbildung 8. Erstellen der vertrauenswürdigen Zone

6.3.1. Ausnahmeregeln

Eine *Ausnahmeregel* ist eine Kombination von Bedingungen, bei deren Vorhandensein ein Objekt nicht von dem Programm Kaspersky Internet Security untersucht wird.

Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm), Prozesse oder Objekte entsprechend der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden.

Klassifikation bedeutet den Status, der einem Objekt bei der Untersuchung von der Anwendung Kaspersky Internet Security zugewiesen wird. Der Status beruht auf der Klassifikation schädlicher und potentiell gefährlicher Programme, die in der Viren-Enzyklopädie von Kaspersky Lab enthalten ist.

Ein potentiell gefährliches Programm besitzt keine schädliche Funktion, kann aber von einem Schadprogramm als Hilfskomponente benutzt werden, weil es Schwachstellen und Fehler enthält. Zu dieser Kategorie gehören beispielsweise Programme zur entfernten Verwaltung, IRC-Clients, FTP-Server, alle

Hilfsprogramme zum Beenden von Prozessen und zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl auf kostenpflichtige Seiten usw. Solche Software wird nicht als Virus klassifiziert (not-a-virus), lässt sich aber beispielsweise in folgende Typen unterteilen: Adware, Joke, Riskware u.a. (ausführliche Informationen über potentiell gefährliche Programme, die von Kaspersky Internet Security entdeckt werden können, finden Sie in der Viren-Enzyklopädie auf der Seite www.viruslist.de). Derartige Programme können aufgrund der Untersuchung gesperrt werden. Da bestimmte Programme, die eine potentielle Gefahr darstellen, von vielen Benutzern verwendet werden, besteht die Möglichkeit, sie von der Untersuchung auszuschließen. Dazu muss der Name oder die Maske des Objekts entsprechend der Klassifikation der Viren-Enzyklopädie zur vertrauenswürdigen Zone hinzugefügt werden.

Es kann beispielsweise sein, dass Sie häufig mit dem Programm Remote Administrator arbeiten. Dabei handelt es sich um ein System, das dem entfernten Zugriff dient und die Arbeit auf einem entfernten Computer erlaubt. Diese Anwendungsaktivität wird von Kaspersky Internet Security als potentiell gefährlich eingestuft und kann blockiert werden. Um zu verhindern, dass das Programm gesperrt wird, muss eine Ausnahmeregel erstellt werden, in der not-a-virus:RemoteAdmin.Win32.RAdmin.22 als Klassifikation genannt wird.

Beim Hinzufügen einer Ausnahme wird eine Regel erstellt, die danach für mehrere Programmkomponenten (Datei-Anti-Virus, Mail-Anti-Virus, Proaktiver Schutz) sowie bei der Ausführung von Aufgaben zur Virensuche verwendet werden kann. Eine Ausnahmeregel kann entweder in dem dafür vorgesehenen Fenster erstellt werden, das aus dem Konfigurationsfenster des Programms geöffnet wird, oder aus der Meldung über den Fund eine Objekts, sowie aus dem Berichtsfenster.

Hinzufügen einer Ausnahme zu den ***Regeln für Ausnahmen****:*

1. Klicken Sie auf der Registerkarte **Regeln für Ausnahmen** auf die Schaltfläche **Hinzufügen**.
2. Legen Sie im folgenden Fenster (s. Abb. 9) im Abschnitt **Parameter** den Typ der Ausnahme fest:

   - ☑ **Objekt** – Ein bestimmtes Objekt, ein Ordner oder Dateien, die einer bestimmten Maske entsprechen, werden von der Untersuchung ausgeschlossen.
   - ☑ **Verdikt** – Ein Objekt wird von der Untersuchung ausgeschlossen, wobei sein Status entsprechend der Klassifikation der Viren-Enzyklopädie zugrunde gelegt wird.

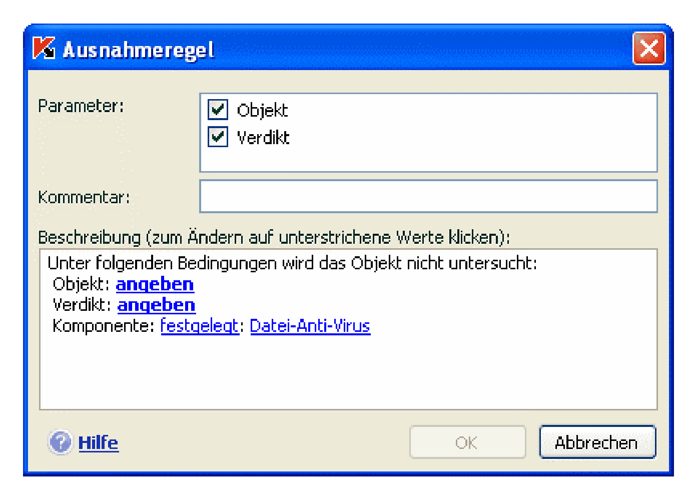


Abbildung 9. Erstellen einer Ausnahmeregel

Wenn gleichzeitig beide Kontrollkästchen angekreuzt werden, wird eine Regel für das angegebene Objekt mit einem bestimmten Status nach der Klassifikation der Viren-Enzyklopädie erstellt. In diesem Fall gelten folgende Regeln:

- Wenn als **Objekt** eine bestimmte Datei festgelegt wird und als **Verdikt** ein bestimmter Status, dann wird die gewählte Datei nur dann ausgeschlossen, wenn ihr bei der Untersuchung der Status der festgelegten Bedrohung zugewiesen wurde.

- Wenn als **Objekt** ein bestimmter Bereich oder ein Ordner angegeben wird und als **Verdikt** ein Status (oder eine Maske), dann werden nur Objekte des gewählten Status von der Untersuchung ausgeschlossen, die im festgelegten Bereich bzw. Ordner gefunden wurden.

3. Legen Sie Werte für die gewählten Ausnahmetypen fest. Klicken Sie dazu im Abschnitt **Beschreibung** mit der linken Maustaste auf den Link angeben, der sich neben dem Typ der Ausnahme befindet:

   - Geben Sie für den Typ **Objekt** im folgenden Fenster den Namen des Objekts an (dabei kann es sich um eine Datei, ein bestimmtes Verzeichnis oder eine Dateimaske handeln (s. Anhang A.2 auf S. 331). Aktivieren Sie das Kontrollkästchen **Unterordner einschließen**, damit das festgelegte Objekt (Datei, Dateimaske, Verzeichnis) bei der Untersuchung rekursiv ausgeschlossen wird. Wenn Sie beispielsweise die Datei **C:\Programme\winword.exe** als Ausnahme festgelegt und das Kontrollkästchen für die Untersuchung von Unterordnern

aktiviert haben, wird die Datei **winword.exe** von der Untersuchung ausgeschlossen, die sich in einem beliebigen Ordner des Verzeichnisses **C:\Programme** befinden kann.

- Geben Sie als **Verdikt** den vollständigen Namen der von der Untersuchung auszuschließenden Bedrohung an, wie er in der Viren-Enzyklopädie genannt wird, oder den Namen nach einer Maske (s. Anhang A.3 auf S. 332).

  Für einige Klassifikationsobjekte können im Feld **Erweiterte Einstellungen** zusätzliche Bedingungen für die Verwendung der Ausnahme festgelegt werden (s. Pkt. A.3 auf S. 332). In den meisten Fällen wird dieses Feld automatisch ausgefüllt, wenn eine Ausnahmeregel aus der Meldung des Proaktiven Schutzes hinzugefügt wird.

  Die Angabe von zusätzlichen Parametern kann beispielsweise für folgende Verdikte notwendig sein:

  - *Invader* (Eindringen in Programmprozesse). Für dieses Verdikt können Sie als zusätzliche Bedingung den Namen, die Maske oder den vollständigen Pfad des Zielobjekts angeben (z.B. der dll-Datei).

  - *Launching Internet Browser* (Browserstart mit Parametern) Für dieses Verdikt können Sie als zusätzliche Bedingung die Parameter für den Browserstart angeben. Beispielsweise haben Sie im Proaktiven Schutz bei der Aktivitätsanalyse von Anwendungen den Browserstart mit Parametern verboten, möchten aber als Ausnahmeregel den Browserstart für die Domäne *www.kasperky.com* mit einem Link aus Microsoft Office Outlook erlauben. Geben Sie dazu als **Objekt** der Ausnahme das Programm Microsoft Office Outlook, als **Verdikt** *Launching Internet Browser* und im Feld **Erweiterte Einstellungen** die Maske der erlaubten Domäne an.

4. Legen Sie fest, für welche Komponenten von Kaspersky Internet Security die neue Regel bei der Arbeit verwendet werden soll. Bei Auswahl des Werts beliebige wird diese Regel für alle Komponenten übernommen. Wenn Sie die Verwendung der Regel auf eine oder mehrere Komponenten beschränken möchten, klicken Sie auf den Link beliebige. Der Link ändert sich in festgelegte. Durch Klick auf den Link angeben wird ein weiteres Fenster geöffnet. Aktivieren Sie dort die Kontrollkästchen der Komponenten, für welche diese Ausnahmeregel gelten soll.

Hinzufügen einer Ausnahmeregel aus der Programmmeldung über den Fund eines gefährlichen Objekts:

1. Verwenden Sie im Meldungsfenster (s. Abb. 10) den Link Zur vertrauenswürdigen Zone hinzufügen.



Abbildung 10. Meldung über den Fund eines gefährlichen Objekts

2. Überprüfen Sie im folgenden Fenster, ob alle Parameter der Ausnahmeregel korrekt sind. Die Felder mit dem Objektnamen und dem zugewiesenen Bedrohungstyp werden aufgrund der Informationen aus der Meldung automatisch ausgefüllt. Klicken Sie auf **OK**, um die Regel zu erstellen.

Erstellen einer Ausnahmeregel vom Berichtsfenster aus:

1. Wählen Sie im Bericht das Objekt aus, das Sie zu den Ausnahmen hinzufügen möchten.
2. Öffnen Sie das Kontextmenü und wählen Sie den Punkt **Zur vertrauenswürdigen Zone hinzufügen** (s. Abb. 11).
3. Dadurch wird das Fenster zur Konfiguration der Ausnahme geöffnet. Überprüfen Sie, ob alle Parameter der Ausnahmeregel korrekt sind. Die Felder mit dem Objektnamen und dem zugewiesenen Bedrohungstyp werden automatisch ausgefüllt, wozu Informationen aus dem Bericht dienen. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu erstellen.

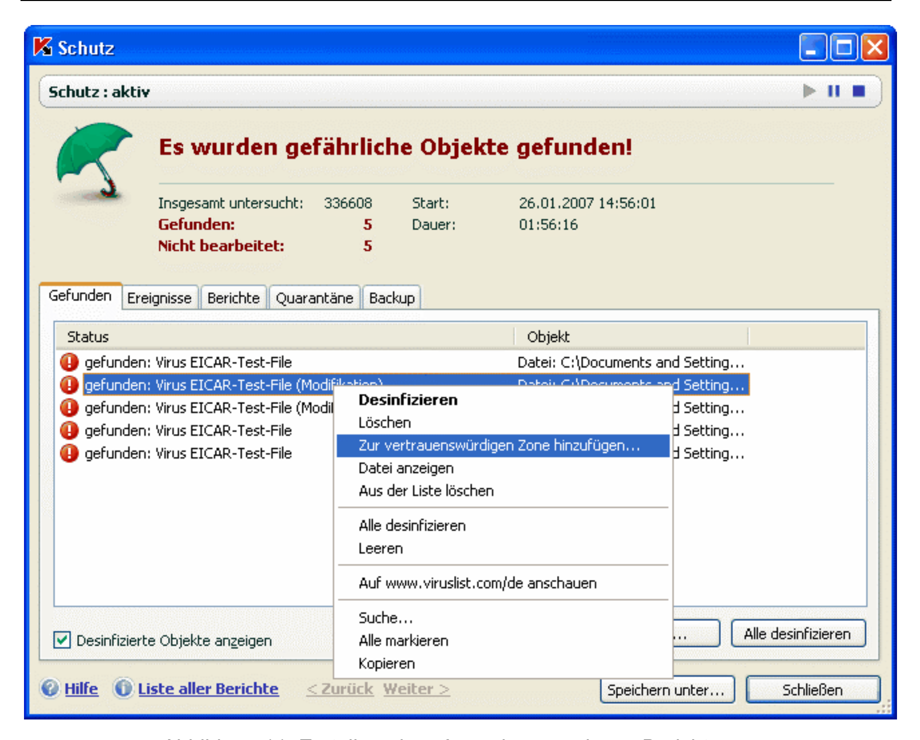


Abbildung 11. Erstellen einer Ausnahmeregel vom Bericht aus

6.3.2. Vertrauenswürdige Anwendungen

Die Option zum Ausschließen vertrauenswürdiger Anwendungen von der Untersuchung ist nur verfügbar, wenn Kaspersky Internet Security auf einem Computer mit dem Betriebssystem Microsoft Windows NT 4.0/2000/XP/Vista installiert ist.

Kaspersky Internet Security erlaubt es, eine Liste von vertrauenswürdigen Anwendungen zu erstellen, deren Aktivität (einschließlich verdächtiger Aktivität, Datei- und Netzwerkaktivität und Zugriff auf die Systemregistrierung) nicht kontrolliert werden soll.

Wenn Sie beispielsweise die Objekte, die von dem standardmäßigen Microsoft Windows-Programm **Editor** verwendet werden, für ungefährlich und deren Untersuchung im Echtzeitschutz nicht für erforderlich halten, bedeutet das, dass Sie diesem Programm vertrauen. Um die Objekte, die von diesem Prozess benutzt werden, von der Untersuchung auszuschließen, fügen Sie das

Programm **Editor** zur Liste der vertrauenswürdigen Anwendungen hinzu. Trotzdem werden aber die ausführbare Datei und der Prozess einer vertrauenswürdigen Anwendung weiterhin auf Viren untersucht. Um eine Anwendung vollständig von der Untersuchung auszuschließen, müssen die Ausnahmeregeln verwendet werden (s. Pkt. 6.3.1 auf S. 80).

Einige Aktionen, die als gefährlich klassifiziert werden, sind im Rahmen der Funktionalität bestimmter Programme normal. Beispielsweise ist das Abfangen eines Texts, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (Punto Switcher u.ä.) eine normale Aktion. Um die Besonderheit solcher Programme zu berücksichtigen und die Kontrolle ihrer Aktivität abzuschalten, empfehlen wir, sie in die Liste der vertrauenswürdigen Anwendungen aufzunehmen.

Das Ausschließen vertrauenswürdiger Anwendungen aus der Untersuchung erlaubt es außerdem, mögliche Kompatibilitätsprobleme von Kaspersky Internet Security mit anderen Anwendungen zu lösen (wenn beispielsweise der Netzwerkverkehr von einem anderen Computer bereits von einer Antiviren-Anwendung untersucht wurde). Außerdem lässt sich auf diese Weise die Leistungsfähigkeit des Computers erhöhen, was insbesondere bei Serveranwendungen wichtig ist.

Kaspersky Internet Security untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden sollen, und kontrolliert die Aktivität aller Programme und den von ihnen erzeugten Netzwerkverkehr.

Die Liste der vertrauenswürdigen Anwendungen erfolgt auf der speziellen Registerkarte **Vertrauenswürdige Anwendungen** (s. Abb. 12). Diese Liste enthält bei der Installation von Kaspersky Internet Security standardmäßig Anwendungen, deren Aktivität aufgrund von Empfehlungen der Kaspersky-Lab-Spezialisten nicht analysiert wird. Wenn Sie eine in der Liste enthaltene Anwendung für nicht vertrauenswürdig halten, deaktivieren Sie das entsprechende Kontrollkästchen. Sie können die Liste mit Hilfe der rechts angebrachten Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** bearbeiten.

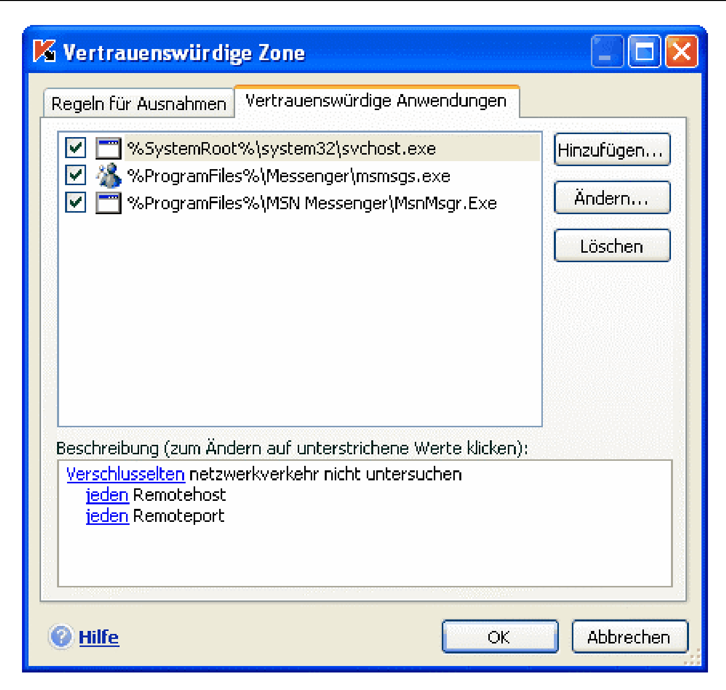


Abbildung 12. Liste der vertrauenswürdigen Anwendungen

Um ein Programm zur Liste der vertrauenswürdigen Anwendungen hinzuzufügen:

1. Klicken Sie auf der rechten Seite des Fensters auf die Schaltfläche **Hinzufügen**.
2. Das Fenster **Vertrauenswürdige Anwendung** (s. Abb. 13) wird geöffnet. Klicken Sie zur Auswahl der Anwendung auf die Schaltfläche **Durchsuchen**. Dadurch öffnet sich ein Kontextmenü, in dem Sie mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl gelangen und den Pfad der ausführbaren Datei angeben können, oder mit dem Punkt **Anwendungen** zur Liste der momentan aktiven Anwendungen wechseln können, um die gewünschte auszuwählen.

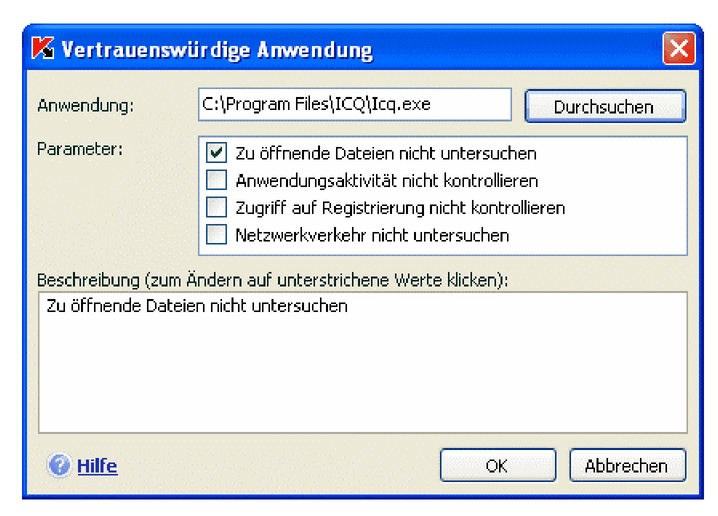


Abbildung 13. Hinzufügen einer Anwendung zur Liste der vertrauenswürdigen Anwendungen

Bei der Auswahl eines Namens speichert Kaspersky Internet Security die internen Attribute der ausführbaren Datei, mit denen das Programm bei der Untersuchung als vertrauenswürdig identifiziert wird.

Der Pfad der Datei wird bei der Auswahl des Namens automatisch ergänzt.

3. Geben Sie nun die von diesem Prozess ausführbaren Aktionen an, die von Kaspersky Internet Security nicht kontrolliert werden sollen:

   ☑ **Zu öffnende Dateien nicht untersuchen** – alle Dateien von der Untersuchung ausschließen, die von dem Prozess der vertrauenswürdigen Anwendung geöffnet werden.

   ☑ **Anwendungsaktivität nicht kontrollieren** – Im Rahmen der Arbeit der Komponente Proaktiver Schutz soll jede beliebige Aktivität (einschließlich verdächtiger), die von der vertrauenswürdigen Anwendung ausgeführt wird, von der Untersuchung ausgeschlossen werden.

   ☑ **Zugriff auf Registrierung nicht kontrollieren** – Die von vertrauenswürdigen Anwendungen initiierten Versuche zum Zugriff auf die Systemregistrierung werden von der Untersuchung ausgeschlossen.

   ☑ **Netzwerkverkehr nicht untersuchen** – Den Netzwerkverkehr, der von einer vertrauenswürdigen Anwendung initiiert wird, aus der

Viren- und Spam-Untersuchung ausschließen. Sie können entweder den gesamten Netzwerkverkehr einer Anwendung oder nur den (unter Verwendung des SSL-Protokolls) verschlüsselten Verkehr von der Untersuchung ausschließen. Klicken Sie dazu auf den Link Gesamten, der dann den Wert Verschlüsselten annimmt. Außerdem können Sie eine Ausnahme auf einen bestimmten Remotehost/Remoteport beschränken. Klicken Sie zur Angabe der Beschränkung auf den Link beliebiger, der sich dadurch in festgelegter ändert, und geben Sie den Wert des Remotehosts bzw. Remoteports an.

Beachten Sie, dass sich das aktivierte Kontrollkästchen **Netzwerkverkehr nicht untersuchen** nur auf die Viren- und Spam-Untersuchung des Datenverkehrs der betreffenden Anwendung bezieht. Diese Option besitzt keinen Einfluss auf die Datenverkehrsuntersuchung durch die Komponente Anti-Hacker, nach deren Einstellungen die Netzwerkaktivität dieser Anwendung analysiert wird.

6.4. Start von Untersuchungs- und Updateaufgaben mit Rechten eines anderen Benutzers

Beachten Sie, dass diese Option für das Betriebssystem Microsoft Windows 98/ME nicht zur Verfügung steht.

In Kaspersky Internet Security 6.0 ist ein Dienst zum Aufgabenstart unter einem anderen Benutzerkonto (Impersonalisierung) realisiert. Dieser Dienst ist standardmäßig deaktiviert und Aufgaben werden unter dem aktiven Benutzerkonto gestartet, mit dem Sie sich am System angemeldet haben.

Beispielsweise können beim Ausführen einer Untersuchungsaufgabe Zugriffsrechte für das zu untersuchende Objekt erforderlich sein. Dann können Sie diesen Dienst benutzen, um den Aufgabenstart unter dem Namen eines Benutzers zu starten, der über die erforderlichen Privilegien verfügt.

Das Programmupdate kann aus einer Quelle erfolgen, auf die Sie keinen Zugriff (beispielsweise ein Netzwerkverzeichnis für Updates) oder keine Rechte eines autorisierten Proxyserverbenutzers besitzen. In diesem Fall können Sie den Dienst benutzen, um das Programmupdate unter dem Namen eines Benutzers mit entsprechender Berechtigung zu starten.

Um den Aufgabenstart unter einem anderen Benutzerkonto festzulegen,

1. Wählen Sie im Abschnitt **Virensuche** (**Service**) des Hauptfensters den Namen der Aufgabe aus und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Aufgabe.
2. Klicken Sie im Konfigurationsfenster auf die Schaltfläche **Einstellungen** und gehen Sie im folgenden Fenster auf die Registerkarte **Erweitert** (s. Abb. 14).

Aktivieren Sie das Kontrollkästchen **Aufgabenstart mit anderem Benutzernamen**, um diesen Dienst einzuschalten. Geben Sie darunter das Benutzerkonto an, unter dem die Aufgabe gestartet werden soll: Benutzername und Kennwort.

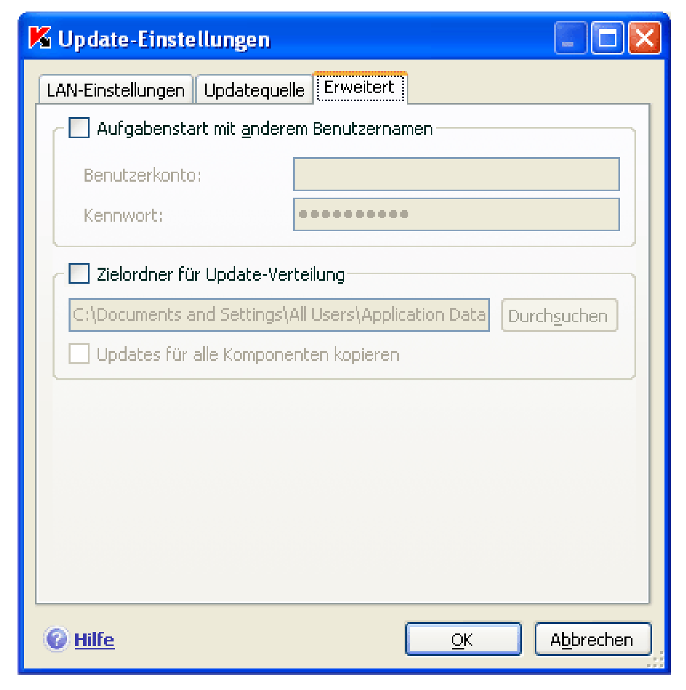


Abbildung 14. Einstellungen für den Start der Updateaufgabe unter einem anderen Benutzerkonto

6.5. Konfiguration des Zeitplans für den Start von Untersuchungs- und Updateaufgaben

Alle Untersuchungs- und Updateaufgaben können manuell oder nach einem festgelegten Zeitplan gestartet werden.

Die Aufgaben zur Virensuche, die bei der Anwendungsinstallation erstellt wurden, werden automatisch nach dem vorgegebenen Zeitplan gestartet. Eine Ausnahme bildet die Untersuchungsaufgabe für Autostart-Objekte, die jedes Mal beim Hochfahren des Computers ausgeführt wird. Der zeitplangesteuerte Start für das Update ist standardmäßig ebenfalls deaktiviert. Er wird automatisch ausgeführt, wenn auf den Kaspersky-Lab-Servern neue Updates vorhanden sind.

Sollten Sie einen anderen Modus für die Arbeit der Aufgaben wünschen, dann ändern Sie die Parameter für ihren automatischen Start. Wählen Sie dazu im Programmhauptfenster im Abschnitt **Virensuche** (für Untersuchungsaufgaben) oder im Abschnitt **Service** (für Updateaufgaben) den Namen der Aufgabe und öffnen Sie mit dem Link Einstellungen das entsprechende Konfigurationsfenster.

Um den zeitplangesteuerten Start einer Aufgabe anzuschalten, aktivieren Sie im Block **Startmodus** das Kontrollkästchen mit der Beschreibung der Bedingungen für den automatischen Aufgabenstart. Die Bedingungen für den Start der Untersuchungsaufgabe können im Fenster **Zeitplan** (s. Abbildung 15) angepasst werden, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.



Abbildung 15. Erstellen eines Zeitplans für den Aufgabenstart

Die wichtigste Einstellung ist die Frequenz für den Aufgabenstart. Folgende Varianten stehen zur Auswahl:

Einmal. Die Aufgabe wird nur einmal an dem von Ihnen angegebenen Tag zur festgelegten Uhrzeit gestartet.

Bei Programmstart. Die Aufgabe wird bei jedem Start von Kaspersky Internet Security gestartet.

Nach jedem Update. Die Aufgabe wird nach jedem Update der Bedrohungssignaturen gestartet (Dieser Punkt bezieht sich nur auf Untersuchungsaufgaben).

Minuten. Das Zeitintervall zwischen den Aufgabenstarts beträgt eine bestimmte Anzahl von Minuten. Geben Sie in den Zeitplaneinstellungen die Anzahl der Minuten zwischen den Starts an. Als Höchstwert gelten 59 Minuten.

Stunden. – Das Intervall zwischen den Aufgabenstarts wird in Stunden festgelegt. Wenn Sie diese Frequenz gewählt haben, geben Sie in den Zeitplaneinstellungen das Intervall **Alle n Stunden** an und bestimmen Sie das Intervall *n*. Wählen Sie beispielsweise für den stündlichen Start *Alle 1 Stunden*.

Tage. – Die Aufgabe wird jeweils nach einer bestimmten Anzahl von Tagen gestartet. Geben Sie in den Zeitplanparametern an, wie oft der Start erfolgen soll:

- Wählen Sie die Variante **Alle n Tage** und geben Sie das Intervall *n* für die Anzahl der Tage an, die zwischen den Aufgabenstarts liegen soll. Geben

Sie beispielsweise *Alle 2 Tage* an, damit die Untersuchung jeden zweiten Tag erfolgt.

- Wählen Sie die Variante **Montag bis Freitag**, wenn die Untersuchung täglich von Montag bis Freitag gestartet werden soll.
- Wählen Sie **Samstag + Sonntag**, damit die Untersuchung nur an Samstagen und Sonntagen erfolgt.

  Geben Sie neben der Frequenz im Feld **Zeit** die Uhrzeit für den Start der Untersuchungsaufgabe an.

Wochen. – Die Untersuchungsaufgabe wird an bestimmten Wochentagen gestartet. Wenn Sie diese Frequenz gewählt haben, aktivieren Sie in den Zeitplaneinstellungen die Kontrollkästchen der Wochentage, an denen die Untersuchung gestartet werden soll. Geben Sie außerdem im Feld *Zeit* die Uhrzeit an, zu der die Untersuchungsaufgabe gestartet werden soll.

Monate – Die Untersuchungsaufgabe wird einmal monatlich zum festgelegten Zeitpunkt gestartet.

Wenn der Start einer Aufgabe aus einem bestimmten Grund übersprungen wurde (wenn beispielsweise der Computer zum betreffenden Zeitpunkt ausgeschaltet war), können Sie festlegen, dass die übersprungene Aufgabe automatisch gestartet wird, sobald dies möglich ist. Aktivieren Sie dazu im Zeitplanfenster das Kontrollkästchen **Übersprungene Aufgabe starten**.

6.6. Leistungseinstellungen

Um sparsam mit der Batterie eines Laptops umzugehen und die Belastung des Prozessors und der Laufwerkssubsysteme zu beschränken, können Sie festlegen, dass Aufgaben zur Virensuche aufgeschoben werden:

- Da die Virensuche auf dem Computer und die Programmaktualisierung relativ viel Ressourcen und Zeit benötigen, empfehlen wir Ihnen, den zeitgesteuerten Start solcher Aufgaben zu deaktivieren. Dadurch können Sie Akkustrom sparen. Bei Bedarf können Sie das Programm selbständig aktualisieren (s. Pkt. 5.6 auf S. 70) oder die Virenuntersuchung starten (s. Pkt. 5.2 auf S. 66). Um den Dienst zum Stromsparen im Batteriebetrieb zu verwenden, aktivieren Sie das Kontrollkästchen **Zeitgesteuerte Aufgaben bei Akkubetrieb nicht starten**.
- Das Ausführen von Untersuchungsaufgaben erhöht die Belastung des Prozessors und der Laufwerkssubsysteme und verlangsamt dadurch die Arbeit anderer Programme. In der Grundeinstellung hält das Programm beim Eintreten dieser Situation die Ausführung von

Untersuchungsaufgaben an und gibt Systemressourcen für Benutzeranwendungen frei.

Allerdings existiert eine Reihe von Programmen, die gestartet werden und im Hintergrundmodus arbeiten, wenn Prozessorressourcen frei werden. Damit die Virenuntersuchung unabhängig von der Arbeit solcher Programme erfolgt, aktivieren Sie das Kontrollkästchen ☑ **Ressourcen für andere Anwendungen freigeben**.

Beachten Sie, dass dieser Parameter für jede Untersuchungsaufgabe individuell angepasst werden kann. In diesem Fall besitzt der für eine konkrete Aufgabe festgelegte Parameter die höchste Priorität.

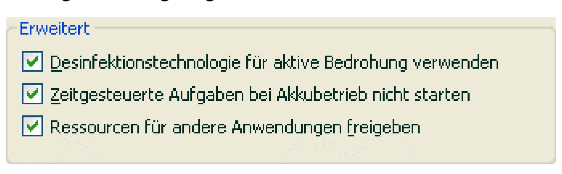


Abbildung 16. Leistungsoptionen

Um die Leistungsoptionen für Untersuchungsaufgaben anzupassen,

wählen Sie den Abschnitt **Schutz** des Anwendungshauptfensters und verwenden Sie den Link Einstellungen. Die Leistungsparameter werden im Block **Erweitert** angepasst (s. Abbildung 16).

6.7. Technologie zur Desinfektion einer aktiven Infektion

Moderne Schadprogramme können auf die tiefsten Ebenen des Betriebssystems vordringen, wodurch es praktisch unmöglich wird, sie zu löschen. Wenn Kaspersky Internet Security eine Bedrohung erkennt, die momentan im System aktiv ist, bietet er an, einen speziell dafür vorgesehenen erweiterten Desinfektionsvorgang auszuführen, durch den die Bedrohung neutralisiert und vom Computer gelöscht wird.

Beim Abschluss des Vorgangs erfolgt der obligatorische Neustart des Computers. Nach dem Neustart des Computers wird empfohlen, die vollständige Virenuntersuchung zu starten. Damit der Vorgang zur erweiterten Desinfektion verwendet wird, aktivieren Sie das Kontrollkästchen ☑ **Desinfektionstechnologie für aktive Bedrohung verwenden**.

Um die Verwendung der Technologie zur Desinfektion einer aktiven Infektion zu aktivieren/ deaktivieren

wählen Sie den Abschnitt **Schutz** des Anwendungshauptfensters und verwenden Sie den Link Einstellungen. Die Leistungsparameter werden im Block **Erweitert** angepasst (s. Abbildung 16).

KAPITEL 7. VIRENSCHUTZ FÜR DAS DATEISYSTEM DES COMPUTERS

Kaspersky Internet Security verfügt über eine spezielle Komponente, die das Dateisystem Ihres Computers vor einer Infektion schützt: *Datei-Anti-Virus.* Die Komponente wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden.

Als Indikator für die Arbeit der Komponente dient das Symbol von Kaspersky Internet Security im Infobereich der Taskleiste, das jedes Mal bei der Untersuchung einer Datei folgendes Aussehen annimmt .

Standardmäßig untersucht Datei-Anti-Virus NUR NEUE oder VERÄNDERTE DATEIEN, d.h. Dateien, die seit dem letzten Zugriff hinzugefügt oder verändert worden sind.

Die Dateiuntersuchung erfolgt nach folgendem Algorithmus:

1. Der Zugriff des Benutzers oder eines bestimmten Programms auf eine beliebige Datei wird von der Komponente abgefangen.

2. Datei-Anti-Virus überprüft, ob die Datenbanken iChecker™ und iSwift™ Informationen über die abgefangene Datei enthalten. Auf Grundlage der ermittelten Informationen wird über die Notwendigkeit der Dateiuntersuchung entschieden.

Der Untersuchungsvorgang umfasst folgende Aktionen:

1. Die Datei wird auf das Vorhandensein von Viren untersucht. Schädliche Objekte werden auf Basis von *Bedrohungssignaturen* erkannt, die bei der Arbeit verwendet werden. Die Signaturen enthalten eine Beschreibung aller momentan bekannten Schadprogramme, Bedrohungen, Netzwerkangriffe und entsprechende Desinfektionsmethoden.

2. Aufgrund der Analyseergebnisse bestehen folgende Varianten für das weitere Vorgehen der Anwendung:

   a. Wenn in der Datei schädlicher Code gefunden wird, sperrt Datei-Anti-Virus die Datei, speichert eine Kopie im *Backup* und versucht, die Datei zu desinfizieren. Bei erfolgreicher

Desinfektion wird die Datei zum Zugriff freigegeben. Wenn die Desinfektion fehlschlägt, wird die Datei gelöscht.

b. Wenn in der Datei ein Code gefunden wird, der Ähnlichkeit mit schädlichem Code besitzt, jedoch keine hundertprozentige Sicherheit darüber besteht, erfolgt ein Desinfektionsversuch und die Datei wird in den Quarantäne-Speicher verschoben.

c. Wenn in der Datei kein schädlicher Code gefunden wird, wird sie sofort zum Zugriff freigegeben.

7.1. Auswahl der Sicherheitsstufe für den Dateischutz

Datei-Anti-Virus bietet Schutz für die Dateien, mit denen Sie arbeiten. Dafür stehen folgende Sicherheitsstufen zur Auswahl (s. Abb. 17):

- **Hoch** – Auf dieser Stufe erfolgt die Kontrolle über Dateien, die geöffnet, gespeichert und gestartet werden, mit maximaler Ausführlichkeit.
- **Empfohlen**. Die Parameter dieser Stufe werden von Kaspersky-Lab-Experten empfohlen und umfassen die Untersuchung folgender Objektkategorien:
    - Programm und Objekte nach ihrem Inhalt
    - nur neue und seit der letzten Objektuntersuchung veränderte Objekte
    - eingebettete OLE-Objekte
- **Niedrig** – Diese Stufe erlaubt Ihnen, komfortabel mit Anwendungen zu arbeiten, die den Arbeitsspeicher stark beanspruchen, weil die Auswahl der untersuchten Dateien auf dieser Stufe eingeschränkt wird.

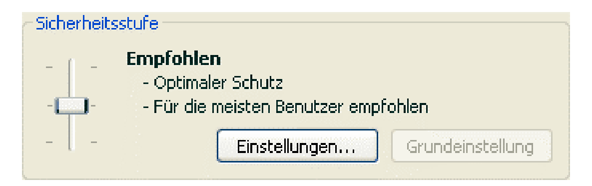


Abbildung 17. Sicherheitsstufe von Datei-Anti-Virus

Der Dateischutz erfolgt standardmäßig auf der **Empfohlenen** Stufe.

Sie können die Schutzstufe für Dateien, mit denen Sie arbeiten, erhöhen oder senken, indem Sie eine andere Stufe wählen oder die Einstellungen der aktuellen Stufe ändern.

Um die Sicherheitsstufe zu ändern,

> verschieben Sie den Zeiger auf der Skala. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Dateien bestimmt: Je weniger Dateien der Virusanalyse unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn keine der vordefinierten Stufen für den Dateischutz Ihren Anforderungen entspricht, können Sie die Schutzparameter zusätzlich anpassen. Wählen Sie dazu die Stufe, die Ihren Anforderungen am nächsten kommt, als Ausgangsstufe und ändern Sie ihre Parameter entsprechend. In diesem Fall ändert sich die Stufe in **Benutzerdefiniert**. Betrachten wir ein Beispiel, in dem die benutzerdefinierte Sicherheitsstufe für den Dateischutz nützlich sein kann.

Beispiel:

> Aufgrund von Besonderheiten Ihrer Tätigkeit arbeiten Sie mit einer großen Menge von Dateien unterschiedlicher Typen, darunter auch relativ umfangreiche Dateien. Sie möchten es nicht riskieren, Dateien entsprechend der Namenserweiterung oder Größe von der Untersuchung auszuschließen, selbst wenn dadurch die Leistungsfähigkeit Ihres Computers beeinflusst wird.

Empfehlung zur Auswahl der Stufe:

> Die Analyse der Situation lässt darauf schließen, dass die Infektionsgefahr durch ein Schadprogramm im beschriebenen Beispiel sehr groß ist. Größe und Typ von bei der Arbeit verwendeten Dateien sind sehr vielfältig, weshalb das Festlegen solcher Ausnahmen ein Risiko für die Daten auf dem Computer darstellt. Ein wichtiger Aspekt der Untersuchung besteht in der Analyse von bei der Arbeit verwendeten Dateien nach ihrem Inhalt und nicht nach der Erweiterung.
>
> Es wird empfohlen, die vordefinierte Schutzstufe **Empfohlen** folgendermaßen anzupassen: Die Größenbeschränkung für zu untersuchende Dateien wird deaktiviert. Die Arbeit von Datei-Anti-Virus wird dadurch optimiert, dass nur neue und veränderte Dateien untersucht werden. Dadurch wird die Belastung des Computers bei der Dateiuntersuchung gesenkt, was die komfortable Arbeit mit anderen Anwendungen erlaubt.

Um die Einstellungen der aktuellen Sicherheitsstufe anzupassen,

> klicken Sie im Konfigurationsfenster von Datei-Anti-Virus auf die Schaltfläche **Einstellungen**, passen Sie im folgenden Fenster die Einstellungen für den Dateischutz an und klicken Sie auf **OK**.

Dadurch wird eine vierte Sicherheitsstufe mit der Bezeichnung **Benutzerdefiniert** erstellt, welche die von Ihnen definierten Schutzparameter enthält.

7.2. Konfiguration des Dateischutzes

Die Einstellungen, nach denen der Dateischutz auf Ihrem Computer erfolgt, lassen sich in folgende Gruppen aufteilen:

- Parameter, welche die Typen der Dateien festlegen, die der Virusanalyse unterzogen werden (s. Pkt. 7.2.1 auf S. 99).
- Parameter, die den geschützten Bereich festlegen (s. Pkt. 7.2.2 auf S. 102).
- Parameter, welche die Aktion für ein gefährliches Objekt festlegen (s. Pkt. 7.2.5 auf S. 107).
- zusätzliche Parameter für die Arbeit von Datei-Anti-Virus (s. Pkt. 7.2.3 auf S. 104).

In diesem Abschnitt des Handbuchs werden alle oben genannten Gruppen ausführlich beschrieben.

7.2.1. Festlegen der Typen von zu untersuchenden Dateien

Durch die Angabe des Typs der zu untersuchenden Dateien definieren Sie das Format, die Größe und die Laufwerke der Dateien, die beim Öffnen, Ausführen und Speichern auf Viren untersucht werden sollen.

Zur Vereinfachung der Konfiguration werden alle Dateien in zwei Gruppen eingeteilt: *einfache* und *zusammengesetzte*. Einfache Dateien enthalten kein anderes Objekt (z.B. eine txt-Datei). Zusammengesetzte Objekte können mehrere Objekte umfassen, die wiederum jeweils mehrere Anhänge enthalten können. Hierfür gibt es viele Beispiele: Archive, Dateien, die Makros, Tabellen, Nachrichten mit Anlagen usw. enthalten.

Der Dateityp für die Virusanalyse wird im Abschnitt **Dateitypen** (s. Abb. 18) festgelegt. Wählen Sie eine der drei Varianten:

Alle Dateien untersuchen. In diesem Fall werden alle Objekte des Dateisystems, die geöffnet, gestartet und gespeichert werden ohne Ausnahmen der Analyse unterzogen.

◉ **Programme und Dokumente (nach Inhalt) untersuchen**. Bei der Auswahl dieser Dateigruppe untersucht Datei-Anti-Virus nur potentiell infizierbare Dateien, d.h. Dateien, in die ein Virus eindringen kann.

> Hinweis.
>
> Es gibt eine Reihe von Dateiformaten, für die das Risiko des Eindringens von schädlichem Code und der späteren Aktivierung relativ gering ist. Dazu zählen beispielsweise Dateien im *txt*-Format.
>
> Im Gegensatz dazu gibt es Dateiformate, die ausführbaren Code enthalten oder enthalten können. Als Beispiele für solche Objekte dienen Dateien der Formate *exe*, *dll*, *doc*. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

Bevor die Virensuche in einer Datei beginnt, wird die interne Kopfzeile der Datei hinsichtlich des Dateiformats untersucht (txt, doc, exe usw.). Wenn sich aufgrund der Analyse ergibt, dass eine Datei dieses Formats nicht infiziert werden kann, dann wird sie nicht auf Viren untersucht und sofort für den Zugriff freigegeben. Besteht aber aufgrund des Dateiformats für einen Virus die Möglichkeit des Eindringens, dann wird die Datei auf Viren untersucht.

◉ **Programme und Dokumente (nach Erweiterung) untersuchen**. In diesem Fall untersucht Datei-Anti-Virus nur potentiell infizierbare Dateien, wobei das Format auf Basis der Dateinamenserweiterung ermittelt wird. Wenn Sie dem Link Erweiterung folgen, gelangen Sie zu einer Liste der Dateierweiterungen (s. Anhang A.1 auf S. 329), die in diesem Fall untersucht werden.

> Hinweis.
>
> Es sollte beachtet werden, dass ein Angreifer einen Virus in einer Datei mit der Erweiterung txt an Ihren Computer senden kann, obwohl es sich in Wirklichkeit um eine ausführbare Datei handelt, die in eine txt-Datei umbenannt wurde. Wenn Sie die Variante ◉ **Programme und Dokumente (nach Erweiterung) untersuchen** wählen, wird eine solche Datei bei der Untersuchung übersprungen. Wenn Sie die Variante ◉ **Programme und Dokumente (nach Inhalt) untersuchen** gewählt haben, analysiert Datei-Anti-Virus ungeachtet der Erweiterung die Kopfzeile der Datei, wodurch sich ergibt, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.



Abbildung 18. Auswahl der Dateitypen, die der Virenuntersuchung unterzogen werden sollen

Im Abschnitt **Optimierung** lässt sich festlegen, dass nur Dateien untersucht werden sollen, die neu sind oder seit ihrer letzten Untersuchung verändert wurden. Dieser Modus erlaubt es, die Untersuchungszeit wesentlich zu verkürzen und die Arbeitsgeschwindigkeit des Programms zu erhöhen. Aktivieren Sie dazu das Kontrollkästchen ☑ **Nur neue und veränderte Dateien untersuchen**. Dieser Modus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Geben Sie im Abschnitt **Zusammengesetzte Dateien** an, welche zusammengesetzten Dateien auf Viren untersucht werden sollen:

☑ **<u>Alle/Nur neue</u> Archive untersuchen** – Archive der Formate ZIP, CAB, RAR, ARJ untersuchen.

☑ **<u>Alle/Nur neue</u> Installationspakete untersuchen** – selbstextrahierende Archive auf Viren untersuchen.

☑ **<u>Alle/Nur neue</u> angehängte(n) OLE-Objekte untersuchen** – Objekte, die in eine Datei eingebettet sind, untersuchen (z.B. eine Excel-Tabelle oder ein Makro, das in eine Datei des Typs Microsoft Office Word eingebettet ist, Anhänge von E-Mail-Nachrichten, usw.).

Für jeden Typ einer zusammengesetzten Datei können sie wählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie dazu den Link neben der Bezeichnung des Objekts. Der Link verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn im Abschnitt **Optimierung** festgelegt wurde, dass nur neue und veränderte Dateien untersucht werden sollen, steht die Auswahl des Typs der zusammengesetzten Dateien nicht zur Verfügung.

Um festzulegen, welche zusammengesetzten Dateien nicht auf Viren untersucht werden sollen, verwenden Sie folgende Parameter:

- **Später extrahieren, wenn Datei größer als ... MB**. Wenn die Größe eines zusammengesetzten Objekts diesen Wert überschreitet, wird es vom Programm wie ein einzelnes Objekt untersucht (Kopfzeile wird analysiert) und dem Benutzer zur Arbeit übergeben. Die Untersuchung der Objekte, die dazu gehören, erfolgt später. Wenn dieses Kontrollkästchen nicht aktiviert ist, wird der Zugriff auf Dateien, die über der angegebenen Größe liegen, bis zum Abschluss der Objektuntersuchung blockiert.
- **Nicht extrahieren, wenn Datei größer als ... MB**. In diesem Fall wird eine Datei mit der angegebenen Größe bei der Virenuntersuchung übersprungen.

7.2.2. Festlegen des Schutzbereichs

Datei-Anti-Virus untersucht standardmäßig alle Dateien, auf die zugegriffen wird, unabhängig davon, auf welchem Datenträger sie sich befinden (Festplatte, CD/DVD-ROM, Flash-Card).

Sie können den Schutzbereich folgendermaßen einschränken:

1. Wählen Sie im Hauptfenster **Datei-Anti-Virus** und wechseln Sie über den Link Einstellungen zum Konfigurationsfenster der Komponente.
2. Klicken Sie auf die Schaltfläche **Einstellungen** und wählen Sie im folgenden Fenster die Registerkarte **Schutzbereich** (s. Abb. 19).

Auf der Registerkarte befindet sich eine Liste der Objekte, die der Untersuchung durch Datei-Anti-Virus unterliegen. Standardmäßig ist der Schutz aller Objekte aktiviert, die sich auf Festplatten, Wechseldatenträgern und Netzwerklaufwerken befinden, die an Ihren Computer angeschlossen sind. Sie können die Liste mit Hilfe der Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** ergänzen oder anpassen.

Wenn Sie den Bereich der zu schützenden Objekte einschränken möchten, können Sie folgendermaßen vorgehen:

1. Nur die Verzeichnisse, Laufwerke oder Dateien angeben, die geschützt werden sollen.

2. Eine Liste der Objekte anlegen, die nicht geschützt werden sollen.

3. Die erste und zweite Methode vereinigen, d.h. einen Schutzbereich erstellen, aus dem bestimmte Objekte ausgeschlossen werden.

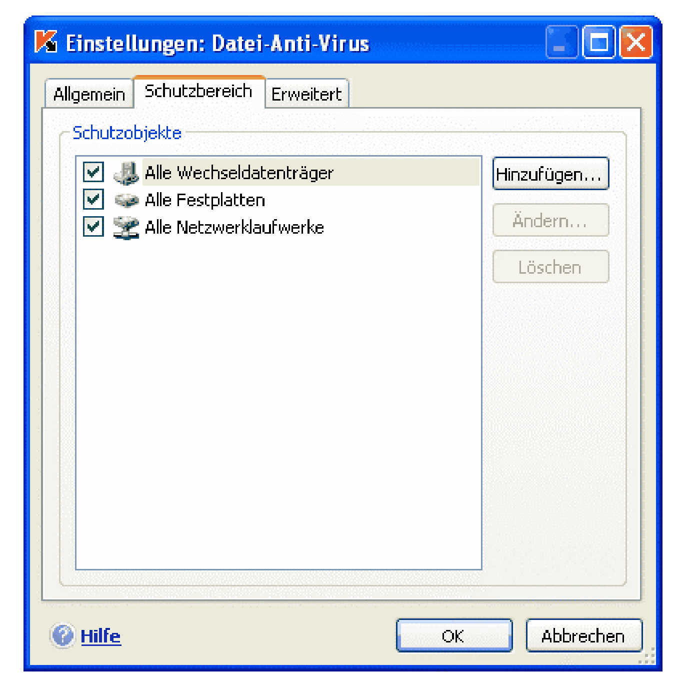


Abbildung 19. Festlegen des Schutzbereichs

Beim Hinzufügen eines Untersuchungsobjekts können Masken verwendet werden. Beachten Sie, dass Masken nur mit den absoluten Pfaden der Objekte angegeben werden dürfen:

- **C:\dir*.*** oder **C:\dir*** oder **C:\dir** – alle Dateien im Ordner *C:\dir*
- **C:\dir*.exe** – alle Dateien mit der Endung *.exe* im Ordner *C:\dir*
- **C:\dir*.ex?** – alle Dateien mit der Endung *.ex?* im Ordner *C:\dir*, wobei anstelle von ? ein beliebiges Zeichen stehen kann.
- **C:\dir\test** – nur die Datei *C:\dir\test*

Damit die rekursive Untersuchung des gewählten Objekts ausgeführt wird, aktivieren Sie das Kontrollkästchen ☑ **Unterordner einschließen**.

Achtung.

Beachten Sie, dass Datei-Anti-Virus nur jene Dateien auf Viren untersucht, die zu dem erstellten Schutzbereich gehören. Dateien, die nicht in diesen Bereich fallen, werden ohne Untersuchung zur Arbeit freigegeben. Dadurch steigt das Risiko einer Infektion Ihres Computers!

7.2.3. Anpassen zusätzlicher Parameter

Als zusätzliche Parameter für Datei-Anti-Virus können Sie den Untersuchungsmodus für die Objekte des Dateisystems festlegen und bestimmen, unter welchen Bedingungen die Arbeit der Komponente vorübergehend angehalten werden soll.

Um die zusätzlichen Parameter von Datei-Anti-Virus anzupassen:

1. Wählen Sie im Hauptfenster die Komponente **Datei-Anti-Virus** aus und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Komponente.
2. Klicken Sie auf die Schaltfläche **Einstellungen** und wählen Sie im folgenden Fenster die Registerkarte **Erweitert** (s. Abb. 20).

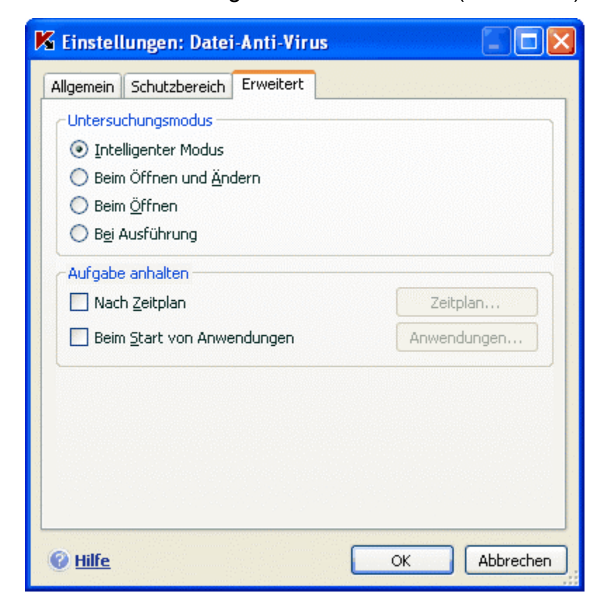


Abbildung 20. Anpassen der zusätzlichen Parameter für Datei-Anti-Virus

Durch den Untersuchungsmodus für Objekte werden die Bedingungen für die Reaktion von Datei-Anti-Virus bestimmt. Folgende Varianten stehen zur Auswahl:

- **Intelligenter Modus**. Dieser Modus dient dazu, die Objektbearbeitung und die Verfügbarkeit von Objekten für den Benutzer zu beschleunigen. Bei der Auswahl dieser Variante wird aufgrund der Analyse der Operationen, die mit einem Objekt ausgeführt werden sollen, über die Untersuchung entschieden.

  Bei der Arbeit mit einem Microsoft Office-Dokument untersucht Kaspersky Internet Security die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

  Der intelligente Untersuchungsmodus wird standardmäßig verwendet.

- **Beim Öffnen und Ändern** – Datei-Anti-Virus untersucht Objekte, wenn sie geöffnet und verändert werden.

- **Beim Öffnen** – Objekte werden nur untersucht, wenn versucht wird, sie zu öffnen.

- **Bei Ausführung** – Objekte werden nur in dem Moment untersucht, wenn versucht wird, sie zu starten.

Das vorübergehende Anhalten von Datei-Anti-Virus kann erforderlich sein, wenn Arbeiten ausgeführt werden, die die Betriebssystemressourcen stark beanspruchen. Um die Belastung zu verringern und den schnellen Zugriff des Benutzers auf Objekte zu gewährleisten, wird empfohlen, das Abschalten der Komponente für einen bestimmten Zeitraum oder bei der Arbeit mit bestimmten Programmen festzulegen.

Damit die Arbeit der Komponente für einen bestimmten Zeitraum angehalten wird, aktivieren Sie das Kontrollkästchen ☑ **Nach Zeitplan** und legen Sie im Fenster (s. Abbildung 6), das mit der Schaltfläche **Zeitplan** geöffnet wird, den Zeitraum fest, für den die Arbeit der Komponente angehalten und nach dem sie fortgesetzt werden soll. Geben Sie in den entsprechenden Feldern die Werte im Format HH:MM ein.



Abbildung 21. Die Arbeit der Komponente anhalten

Damit die Arbeit der Komponente bei der Arbeit mit ressourcenaufwändigen Programmen angehalten wird, aktivieren Sie das Kontrollkästchen ☑ **Beim Start von Anwendungen** und legen Sie im Fenster (s. Abb. 22), das mit der Schaltfläche **Liste** geöffnet wird, die Liste der Programme an.

Verwenden Sie die Schaltfläche **Hinzufügen**, um der Liste eine Anwendung hinzuzufügen. Dadurch wird das Kontextmenü geöffnet. Wechseln Sie entweder mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl und geben Sie die ausführbare Datei der betreffenden Anwendung an oder verwenden Sie den Punkt **Anwendungen**, um zur Liste der momentan aktiven Anwendungen zu gelangen, und wählen Sie dort die gewünschte Anwendung aus.

Um eine Anwendung aus der Liste zu löschen, wählen Sie sie in der Liste aus und klicken Sie auf die Schaltfläche **Löschen**.

Um eine Bedingung für das Anhalten von Datei-Anti-Virus bei der Arbeit einer konkreten Anwendung vorübergehend aufzuheben, ist es ausreichend, das Kontrollkästchen neben dem Namen der Anwendung zu deaktivieren, ohne diese aus der Liste zu löschen.

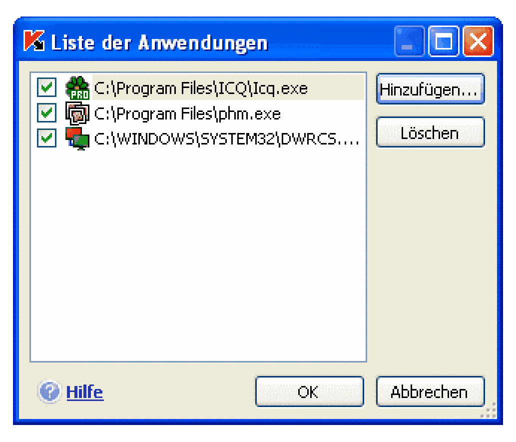


Abbildung 22. Liste der Anwendungen erstellen

7.2.4. Wiederherstellen der Standardparameter für den Dateischutz

Während Sie die Arbeit von Datei-Anti-Virus konfigurieren, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal,

werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Einstellungen für den Dateischutz wiederherzustellen,

1. Wählen Sie im Hauptfenster die Komponente **Datei-Anti-Virus** und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Komponente.

2. Klicken Sie im Abschnitt **Sicherheitsstufe** auf die Schaltfläche **Grundeinstellung**.

Wenn Sie bei der Konfiguration von Datei-Anti-Virus die Liste der Objekte verändert haben, die zum Schutzbereich gehören, wird Ihnen beim Wiederherstellen der ursprünglichen Einstellungen vorgeschlagen, diese Liste zur späteren Verwendung zu speichern. Um die Liste der Objekte beizubehalten, aktivieren Sie im folgenden Fenster **Einstellungen wiederherstellen** das Kontrollkästchen **Schutzbereich**.

7.2.5. Auswahl der Aktion für Objekte

Wenn sich durch die Virenuntersuchung einer Datei herausstellt, dass sie infiziert oder einer Infektion verdächtig ist, hängen die weiteren Operationen von Datei-Anti-Virus vom Status des Objekts und der ausgewählten Aktion ab.

Datei-Anti-Virus kann einem Objekt aufgrund der Untersuchung einen der folgenden Status zuweisen:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*) (s. Pkt. 1.1 auf S. 11).

- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Standardmäßig werden alle infizierten Dateien der Desinfektion unterzogen. Alle möglicherweise infizierten Dateien werden in die Quarantäne verschoben.

Um die Aktion für ein Objekt zu ändern,

wählen Sie im Hauptfenster **Datei-Anti-Virus** und wechseln Sie über den Link Einstellungen in das Konfigurationsfenster der Komponente. Alle verfügbaren Aktionen sind im entsprechenden Abschnitt angegeben (s. Abb. 23).

Aktion
Aktion erfragen
Zugriff verweigern
Desinfizieren
Löschen, wenn Desinfektion nicht möglich

Abbildung 23. Mögliche Aktionen von Datei-Anti-Virus für ein gefährliches Objekt

Gewählte Aktion	Was geschieht beim Fund eines gefährlichen Objekts?
Aktion erfragen	Datei-Anti-Virus zeigt auf dem Bildschirm eine Warnmeldung an, die darüber informiert, von welchem schädlichen Objekt die Datei infiziert bzw. möglicherweise infiziert ist, und bietet Aktionen zur Auswahl an. Die Aktionen können abhängig vom Objektstatus variieren.
Zugriff verweigern	Datei-Anti-Virus blockiert den Zugriff auf das Objekt. Informationen darüber werden im Bericht (s. Pkt. 17.3 auf S. 265) aufgezeichnet. Später kann versucht werden, das Objekt zu desinfizieren.
Zugriff verweigern **Desinfizieren**	Datei-Anti-Virus blockiert den Zugriff auf das Objekt und versucht, es zu desinfizieren. Wenn die Desinfektion des Objekts gelingt, wird der Zugriff freigegeben. Wenn das Objekt nicht desinfiziert werden kann, erhält es den Status *möglicherweise infiziert* und wird in die Quarantäne verschoben (s. Pkt. 17.1 auf S. 258). Informationen darüber werden im Bericht aufgezeichnet. Später kann versucht werden, dieses Objekt zu desinfizieren.

Gewählte Aktion	**Was geschieht beim Fund eines gefährlichen Objekts?**
Zugriff verweigern ☑ **Desinfizieren** ☑ **Löschen, wenn Desinfektion nicht möglich**	Datei-Anti-Virus blockiert den Zugriff auf das Objekt und versucht, es zu desinfizieren. Wenn die Desinfektion des Objekts gelingt, wird der Zugriff freigegeben. Wenn das Objekt nicht desinfiziert werden kann, wird es gelöscht. Dabei wird eine Kopie des Objekts im Backup (s. Pkt. 17.2 auf S. 262) abgelegt.
Zugriff verweigern ☑ **Desinfizieren** ☑ **Löschen**	Datei-Anti-Virus blockiert den Zugriff auf das Objekt und löscht es.

Bevor ein Desinfektionsversuch erfolgt oder das Objekt gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an und speichert diese im Backup. Dadurch wird ermöglicht, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

7.3. Aufgeschobene Desinfektion von Objekten

Wenn Sie als Aktion für schädliche Objekte **Zugriff verweigern** gewählt haben, dann erfolgt für diese keine Desinfektion und der Zugriff wird gesperrt.

Wenn Sie als Aktion

Zugriff verweigern

☑ **Desinfizieren**

gewählt haben, dann werden alle Objekte, deren Desinfektion nicht möglich ist, gesperrt.

Um erneut Zugriff auf blockierte Objekte zu erhalten, müssen diese vorher desinfiziert werden. Dazu:

1. Wählen Sie im Programmhauptfenster die Komponente **Datei-Anti-Virus** und klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Statistik**.

2. Wählen Sie auf der Registerkarte **Gefunden** die gewünschten Objekte und klicken Sie auf die Schaltfläche **Aktionen** → **Alle desinfizieren**.

Wenn die Desinfektion des Objekts gelingt, wird der Zugriff darauf freigegeben. Kann das Objekt nicht desinfiziert werden, dann wird Ihnen zur Auswahl angeboten, es zu *löschen* oder zu *überspringen*. Beim Überspringen wird die Datei für den Zugriff freigegeben. Allerdings erhöht sich dadurch das Risiko einer Infektion Ihres Computers erheblich. Es wird ausdrücklich davor gewarnt, schädliche Objekte zu überspringen.

KAPITEL 8. E-MAIL-VIRENSCHUTZ

Kaspersky Internet Security enthält eine spezielle Komponente, die den Schutz der ein- und ausgehenden E-Mail vor gefährlichen Objekten gewährleistet: *Mail-Anti-Virus.* Diese Komponente wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle E-Mails der Protokolle POP3, SMTP, IMAP, MAPI[1] und NNTP, sowie im sicheren Modus (SSL) mit den Protokollen POP3 und IMAP.

Als Indikator für die Arbeit der Komponente dient das Symbol von Kaspersky Internet Security im Infobereich der Taskleiste, das jedes Mal bei der Untersuchung einer E-Mail folgendes Aussehen annimmt: .

Der E-Mail-Schutz erfolgt standardmäßig nach folgendem Algorithmus:

1. Jeder Brief, der vom Benutzer empfangen oder gesendet wird, wird von Mail-Anti-Virus abgefangen.

2. Die E-Mail-Nachricht wird in ihre Bestandteile zerlegt: Kopfzeile, Briefkörper, Anhänge.

3. Der Körper und die Anhänge der E-Mail-Nachricht (einschließlich eingebetteter OLE-Objekte) werden auf gefährliche Objekte untersucht. Die Suche nach schädlichen Objekten erfolgt auf Basis der *Bedrohungssignaturen*, die bei der Arbeit des Programms verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus. Die Signaturen enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und Methoden zu deren Desinfektion. Der heuristische Algorithmus erlaubt es, neue Viren zu erkennen, die noch nicht in den Bedrohungssignaturen beschrieben sind.

4. Aufgrund der Virenuntersuchung bestehen folgende Varianten für das weitere Vorgehen:

   - Wenn der Körper oder ein Anhang der Nachricht schädlichen Code enthält, sperrt Mail-Anti-Virus den Brief, speichert eine Kopie des infizierten Objekts im *Backup* und versucht das Objekt zu desinfizieren. Bei erfolgreicher Desinfektion wird dem Benutzer der Zugriff auf den Brief freigegeben. Wenn die

---

[1] Die Untersuchung von E-Mails des MAPI-Protokolls wird mit Hilfe eines speziellen Erweiterungsmoduls in Microsoft Office Outlook und The Bat! ausgeführt.

Desinfektion fehlschlägt, wird das infizierte Objekt aus dem Brief gelöscht. Zudem wird in die Betreffzeile des Briefs ein spezieller Text eingefügt, der darüber informiert, dass der Brief von Kaspersky Internet Security bearbeitet wurde.

- Wenn der Körper oder ein Anhang der Nachricht einen Code enthält, der Ähnlichkeit mit schädlichem Code besitzt, jedoch keine hundertprozentige Sicherheit darüber besteht, wird der verdächtige Teil des Briefs in den *Quarantäne-Speicher* verschoben.
- Wenn im Brief kein schädlicher Code gefunden wird, erhält der Benutzer sofort Zugriff darauf.

Für das Mailprogramm Microsoft Office Outlook ist ein spezielles integriertes Erweiterungsmodul vorgesehen (s. Pkt. 8.2.2 auf S. 117), das die Feineinstellung der E-Mail-Untersuchung erlaubt.

Wenn Sie das Mailprogramm The Bat! verwenden, kann Kaspersky Internet Security zusammen mit anderen Antiviren-Anwendungen benutzt werden. Dabei werden die Regeln zur Bearbeitung des Mailverkehrs (s. Pkt. 8.2.3 auf S. 118) direkt im Programm The Bat! erstellt und besitzen Vorrang gegenüber den Parametern für den E-Mail-Schutz durch Kaspersky Internet Security.

Bei der Arbeit mit anderen Mailprogrammen (einschließlich Microsoft Outlook Express, Mozilla Thunderbird, Eudora, Incredimail) untersucht Mail-Anti-Virus den Mailverkehr der Protokolle SMTP, POP3, IMAP und NNTP bei Empfang bzw. Versand.

> Beachten Sie, dass bei der Arbeit mit dem Mailprogramm Thunderbird E-Mails des Protokolls IMAP nicht auf Viren untersucht werden, wenn Filter verwendet werden, welche die Nachrichten aus dem Ordner **Inbox** verschieben.

8.1. Auswahl der E-Mail-Sicherheitsstufe

Kaspersky Internet Security bietet den Schutz Ihrer Post auf einer der folgenden Stufen (s. Abb. 24):

Hoch – Auf dieser Stufe erfolgt die Kontrolle über ein- und ausgehende E-Mail-Nachrichten mit maximaler Ausführlichkeit. Das Programm untersucht unabhängig von der Untersuchungszeit ausführlich die an Briefe angehängten Objekte, einschließlich Archiven.

Empfohlen - Die Parameter dieser Stufe entsprechen den von Kaspersky-Lab-Experten empfohlenen Einstellungen. Sie umfassen die

Untersuchung der gleichen Objekte wie bei der Stufe **Hoch** unter Ausnahme von angehängten Objekten oder Briefen, deren Untersuchung länger als drei Minuten dauert.

Niedrig – Diese Sicherheitsstufe erlaubt Ihnen, komfortabel mit Anwendungen zu arbeiten, die den Arbeitsspeicher stark beanspruchen, weil die Auswahl der untersuchten E-Mail-Objekte auf dieser Stufe eingeschränkt wird. Auf dieser Stufe wird nur Ihre eingehende Post untersucht, wobei angehängte Archive und Objekte (Briefe), deren Untersuchung länger als drei Minuten dauert, nicht untersucht werden. Es wird empfohlen, diese Stufe zu verwenden, wenn auf dem Computer zusätzliche Mittel zum E-Mail-Schutz installiert sind.

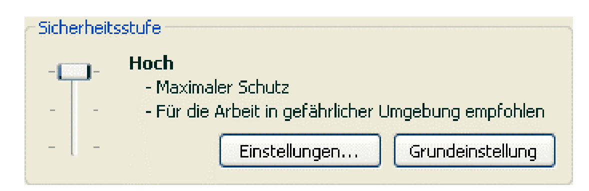


Abbildung 24. Auswahl der Sicherheitsstufe für Mail-Anti-Virus

Der E-Mail-Schutz arbeitet standardmäßig auf der **Empfohlenen** Stufe.

Sie können die Schutzstufe für Ihre Post erhöhen oder senken, indem Sie eine andere Stufe wählen oder die Einstellungen der aktuellen Stufe ändern.

Um die Sicherheitsstufe zu ändern,

verschieben Sie den Zeiger auf der Skala. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Objekte bestimmt: Je weniger E-Mail-Objekte der Analyse auf gefährliche Objekte unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn eine vordefinierte Stufe nicht vollständig Ihren Anforderungen entspricht, können Sie die Parameter zusätzlich anpassen. In diesem Fall ändert sich die Stufe in **Benutzerdefiniert**. Betrachten wir ein Beispiel, in dem die benutzerdefinierte Mail-Sicherheitsstufe nützlich sein kann.

Beispiel:

Ihr Computer befindet sich in einem lokalen Netzwerk und die Internetverbindung erfolgt über ein Modem. Als Mailprogramm zum Empfang und Versand der E-Mail-Korrespondenz wird Microsoft Outlook Express verwendet. Sie verwenden einen kostenlosen E-Mail-Anbieter. Ihre Post enthält aus gewissen Gründen häufig angehängte Archive. Wie lässt sich Ihr Computer optimal vor einer per E-Mail übertragenen Infektion schützen?

Empfehlung zur Auswahl der Stufe:

Die Analyse der Situation lässt darauf schließen, dass die Infektionsgefahr durch ein per E-Mail übertragenes Schadprogramm im beschriebenen Beispiel sehr groß ist (Fehlen eines zentralen E-Mail-Schutzes und Verbindungsmethode zum Internet).

Es wird empfohlen, die vordefinierte Sicherheitsstufe **Hoch** mit folgenden Änderungen zu verwenden: Die Untersuchungszeit für angehängte Objekte wird auf 1-2 Minuten verkürzt. Die Mehrzahl der angehängten Archive wird auf Viren untersucht und die E-Mail-Bearbeitung wird unwesentlich verlangsamt.

Um die Einstellungen einer vordefinierten Sicherheitsstufe anzupassen,

klicken Sie im Konfigurationsfenster für Mail-Anti-Virus auf die Schaltfläche **Einstellungen**, passen Sie im folgenden Fenster die Parameter des E-Mail-Schutzes an und klicken Sie auf **OK**.

8.2. Konfiguration des E-Mail-Schutzes

Die Regeln, nach denen die Untersuchung Ihrer Post erfolgt, werden durch eine Anzahl von Parametern bestimmt. Sie lassen sich in folgende Gruppen aufteilen:

- Parameter, welche die geschützte Richtung der Nachrichten bestimmen (s. Pkt. 8.2.1 auf S. 115).
- Parameter für die E-Mail-Untersuchung in Microsoft Office Outlook (s. Pkt. 8.2.2 auf S. 117) und The Bat! (s. Pkt. 8.2.3 auf S. 118).

> Achtung!
>
> In dieser Version von Kaspersky Internet Security sind keine Mail-Anti-Virus-Erweiterungsmodule für die 64-Bit-Versionen der Mailprogramme vorgesehen.

- Parameter, welche die Aktionen für gefährliche E-Mail-Objekte definieren (s. Pkt. 8.2.5 auf S. 121).

In diesem Abschnitt des Handbuchs werden alle oben genannten Parameter ausführlich beschrieben.

8.2.1. Auswahl der zu schützenden Richtung der Nachrichten

Mail-Anti-Virus erlaubt Ihnen, auszuwählen, in welcher Richtung die E-Mail-Nachrichten auf gefährliche Objekte untersucht werden.

Standardmäßig schützt die Komponente Ihre Post entsprechend der **Empfohlenen** Schutzstufe, d.h. die ein- und ausgehende Post wird untersucht. Zu Beginn der Arbeit mit dem Programm ist es empfehlenswert, die ausgehende Post zu untersuchen, weil die Möglichkeit besteht, dass sich Mailwürmer auf Ihrem Computer befinden, die E-Mails als Kanal verwenden, um sich weiterzuverbreiten. Dadurch wird erlaubt, Probleme zu verhindern, die mit dem unkontrollierten Versenden infizierter E-Mail-Nachrichten von Ihrem Computer verbunden sind.

Wenn Sie sicher sind, dass die von Ihnen gesendeten Briefe keine gefährlichen Objekte enthalten, können Sie die Untersuchung der ausgehenden Post folgendermaßen deaktivieren:

1. Klicken Sie im Konfigurationsfenster für Mail-Anti-Virus auf die Schaltfläche **Einstellungen**.
2. Das Konfigurationsfenster für Mail-Anti-Virus (s. Abbildung 25) wird geöffnet. Wählen Sie die die Variante **Nur eingehende Mails untersuchen** im Block **Schutzbereich**.

Neben der Auswahl der Richtung können Sie festlegen, ob an E-Mails angehängte Archive kontrolliert werden sollen. Außerdem kann die maximale Untersuchungszeit für ein E-Mail-Objekt angepasst werden. Diese Parameter befinden sich im Block **Optimierung**.

Wenn Ihr Computer nicht durch die Mittel eines lokalen Netzwerks geschützt ist und die Internetverbindung ohne Proxyserver oder Firewall erfolgt, wird empfohlen, die Untersuchung angehängter Archive nicht zu deaktivieren und keine Zeitbeschränkung für die Objektuntersuchung festzulegen.

Wenn Sie in einer geschützten Umgebung arbeiten, kann eine Zeitbeschränkung für die Objektuntersuchung festgelegt werden, um das Tempo der E-Mail-Untersuchung zu steigern.

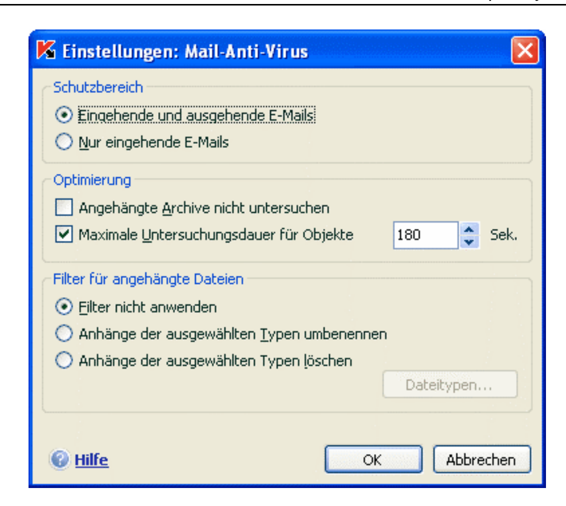


Abbildung 25. Einstellungen für den Schutz des Maildatenstroms

Im Block **Filter für angehängte Dateien** können Sie die Filterbedingungen für an E-Mail-Nachrichten angehängte Objekte festlegen:

- **Filter nicht anwenden** – keine zusätzliche Filterung für Attachments verwenden.
- **Anhänge der genannten Typen umbenennen** – angehängte Dateien eines bestimmten Formats ausfiltern und das letzte Zeichen des Dateinamens durch das Zeichen "Unterstrich" ersetzen. Das Fenster zur Auswahl der Dateitypen wird mit der Schaltfläche **Dateitypen** geöffnet.
- **Anhänge der genannten Typen löschen** – angehängte Dateien eines bestimmten Formats ausfiltern und löschen. Das Fenster zur Auswahl der Dateitypen wird mit der Schaltfläche **Dateitypen** geöffnet.

Details über die Typen der angehängten Dateien, die der Filterung unterzogen werden, finden Sie in Anhang A.1 auf S. 329.

Die Verwendung des Filters bietet Ihrem Computer zusätzliche Sicherheit, da sich Schadprogramme über E-Mails meist in Form angehängter Dateien verbreiten. Das Umbenennen oder Löschen von Attachments eines bestimmten Typs erlaubt es, Ihren Computer beispielsweise davor zu schützen, dass eine angehängte Datei beim Empfang einer Nachricht automatisch geöffnet wird.

8.2.2. Anpassen der E-Mail-Untersuchung in Microsoft Office Outlook

Wenn Sie Microsoft Office Outlook als Mailprogramm verwenden, können Sie die Virenuntersuchung Ihrer Post zusätzlich anpassen.

Bei der Installation von Kaspersky Internet Security wird ein spezielles Erweiterungsmodul in Microsoft Office Outlook integriert. Es erlaubt Ihnen, schnell zu den Einstellungen von Mail-Anti-Virus zu wechseln und festzulegen, zu welchem Zeitpunkt eine E-Mail-Nachricht auf das Vorhandensein gefährlicher Objekte untersucht werden soll.

> Achtung!
>
> In dieser Version von Kaspersky Internet Security ist kein Mail-Anti-Virus-Erweiterungsmodul für die 64-Bit-Version von Microsoft Office Outlook vorgesehen.

Das Erweiterungsmodul besitzt die Form einer speziellen Registerkarte mit dem Namen **Mail-Anti-Virus**, die sich im Menü **Extras** → **Optionen** befindet (s. Abb. 26).

Wählen Sie den Modus für die E-Mail-Untersuchung:

- ☑ **Bei Empfang untersuchen** – Jede E-Mail-Nachricht wird im Moment ihres Eintreffens in Ihrer Mailbox untersucht.
- ☑ **Beim Lesen untersuchen** – E-Mails werden dann untersucht, wenn sie zum Lesen geöffnet werden.
- ☑ **Beim Senden untersuchen** – Jede E-Mail-Nachricht, die Sie senden möchten, wird im Moment des Sendens auf Viren untersucht.

> Achtung!
>
> Wenn Sie zur Verbindung von Microsoft Office Outlook mit dem Mailserver das Protokoll IMAP verwenden, wird empfohlen, den Modus ☑ **Bei Empfang untersuchen** nicht zu benutzen. Wenn dieser Modus aktiviert wird, werden die auf dem Server eintreffenden E-Mails zwangsläufig auf den lokalen Computer kopiert. Dadurch geht der Hauptvorteil des IMAP-Protokolls verloren, der in der Einsparung von Netzwerkverkehr und in der Verwaltung unerwünschter Briefe auf dem Server ohne Kopieren auf den Benutzercomputer besteht.

Die Aktion, die mit gefährlichen E-Mail-Objekten erfolgt, wird in den Einstellungen für Mail-Anti-Virus festgelegt, zu denen Sie über den Link hier wechseln können.

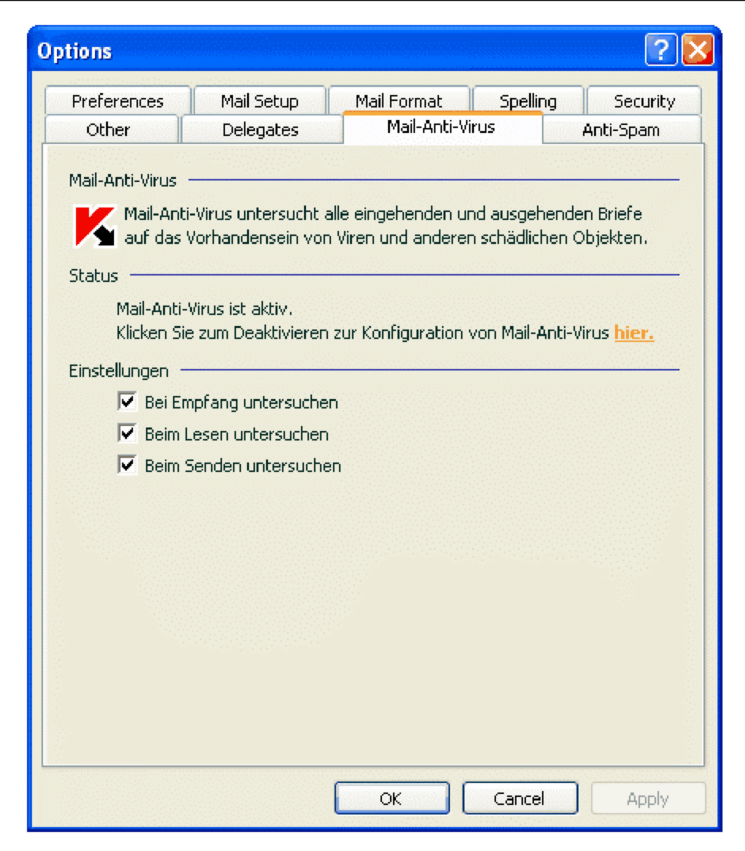


Abbildung 26. Detaillierte Konfiguration des E-Mail-Schutzes in Microsoft Office Outlook

8.2.3. Anpassen der E-Mail-Untersuchung in The Bat!

Die Aktionen für infizierte E-Mail-Objekte werden im Mailprogramm The Bat! durch Mittel des Programms festgelegt.

Achtung!

Die Parameter von Mail-Anti-Virus, die festlegen, ob ein- und ausgehende Post untersucht werden oder nicht, und die Aktionen für gefährliche E-Mail-Objekte und Ausnahmen bestimmen, werden ignoriert. Das Programm The Bat! berücksichtigt lediglich folgende Parameter: Untersuchung angehängter Archive und Zeitbeschränkung für die Untersuchung eines E-Mail-Objekts (s. Pkt. 8.2.1 auf S. 115).

In dieser Version von Kaspersky Internet Security ist kein Mail-Anti-Virus-Erweiterungsmodul für die 64-Bit-Version von The Bat! vorgesehen.

Um in The Bat! die Regeln für die Einstellungen für den Mail-Schutz anzupassen,

1. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.

2. Wählen Sie in der Konfigurationsstruktur den Punkt **Anti-Virus-PlugIns**.

Die hier angezeigten Parameter für den E-Mail-Schutz (s. Abb. 27) gelten für alle auf dem Computer installierten Antivirenmodule, welche die Arbeit mit The Bat! unterstützen.

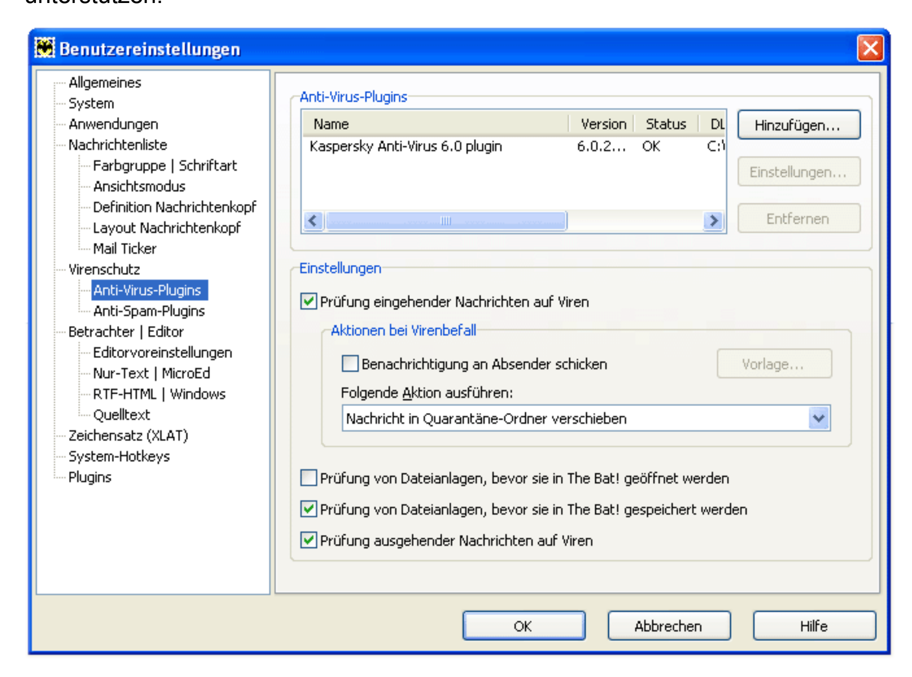


Abbildung 27. Untersuchungseinstellungen in The Bat!

Folgende Einstellungen sind erforderlich:

- Welche Richtung des E-Mail-Verkehrs (eingehende, ausgehende) soll der Virenprüfung unterzogen werden.
- In welchem Moment soll die Virenuntersuchung der E-Mail-Objekte erfolgen (beim Öffnen eines Briefs, vor dem Speichern auf der Festplatte).
- Aktionen, die das Mailprogramm beim Fund gefährlicher Objekte in E-Mail-Nachrichten ausführen soll. Es stehen beispielsweise zur Auswahl:

  Reparaturversuch infizierter Teile – Es wird versucht, das infizierte E-Mail-Objekt zu desinfizieren. Wenn die Desinfektion unmöglich ist, verbleibt das Objekt im Brief. Kaspersky Internet Security benachrichtigt Sie darüber, dass ein Objekt der E-Mail-Nachricht infiziert ist. Doch selbst wenn Sie in der Meldung von Mail-Anti-Virus die Aktion **Löschen** wählen, verbleibt das Objekt in der E-Mail-Nachricht, weil die in The Bat! gewählte Aktion höhere Priorität besitzt, als die Aktion von Mail-Anti-Virus.

  Infizierte Teile löschen – Ein gefährliches E-Mail-Objekt wird gelöscht, wenn es infiziert ist oder als verdächtig gilt.

  Standardmäßig verschiebt das Programm The Bat! alle infizierten E-Mail-Objekte ohne Desinfektion in den Ordner Quarantäne.

Achtung!

E-Mail-Nachrichten, die gefährliche Objekte enthalten, werden von dem Programm The Bat! nicht durch eine spezielle Kopfzeile gekennzeichnet.

8.2.4. Wiederherstellen der Standardparameter für den Mail-Schutz

Während Sie die Arbeit von Mail-Anti-Virus anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Parameter für den Mail-Schutz wiederherzustellen,

1. Wählen Sie die Komponente **Mail-Anti-Virus** im Hauptfenster aus und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Komponente.

2. Klicken Sie im Abschnitt **Sicherheitsstufe** auf die Schaltfläche **Grundeinstellung**.

8.2.5. Auswahl der Aktion für ein gefährliches E-Mail-Objekt

Wenn sich durch die Virenuntersuchung einer E-Mail-Nachricht herausstellt, dass ein Brief oder ein E-Mail-Objekt (Briefkörper, Anhang) infiziert oder verdächtig ist, hängen die weiteren Operationen von Mail-Anti-Virus vom Status des Objekts und der ausgewählten Aktion ab.

Ein E-Mail-Objekt kann aufgrund der Untersuchung einen der folgenden Status erhalten:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*, Details s. Pkt. 1.1 auf S. 11).
- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Standardmäßig zeigt Mail-Anti-Virus beim Fund eines gefährlichen oder möglicherweise infizierten Objekts auf dem Bildschirm eine Warnung an und bietet mehrere Aktionen für das Objekt zur Auswahl an.

Um die Aktion für ein Objekt zu ändern,

öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security und wählen Sie **Mail-Anti-Virus**. Alle verfügbaren Aktionen für gefährliche Objekte werden im Block **Aktion** genannt (s. Abb. 28).



Abbildung 28. Auswahl der Aktion für ein gefährliches E-Mail-Objekt

Betrachten wir die möglichen Varianten zur Bearbeitung gefährlicher E-Mail-Objekte genauer:

Gewählte Aktion	Was geschieht beim Fund eines gefährlichen Objekts?
Aktion erfragen	Mail-Anti-Virus zeigt eine Warnmeldung auf dem Bildschirm an, die darüber informiert, von was für einem schädlichen Objekt die E-Mail infiziert (möglicherweise infiziert) ist, und bietet Aktionen zur Auswahl an.
Zugriff verweigern	Mail-Anti-Virus blockiert den Zugriff auf das Objekt. Informationen darüber werden im Bericht aufgezeichnet (s. Pkt. 17.3 auf S. 265). Später kann versucht werden, das Objekt zu desinfizieren.
Zugriff verweigern **Desinfizieren**	Mail-Anti-Virus blockiert den Zugriff auf das Objekt und versucht, es zu desinfizieren. Wenn das Objekt desinfiziert werden konnte, wird es zur Arbeit freigegeben. Wenn der Desinfektionsversuch erfolglos war, wird das Objekt in die Quarantäne verschoben (s. Pkt. 17.1 auf S. 258). Informationen darüber werden im Bericht aufgezeichnet. Später kann versucht werden, das Objekt zu desinfizieren.
Zugriff verweigern **Desinfizieren** **Löschen, wenn Desinfektion nicht möglich**[2]	Mail-Anti-Virus blockiert den Zugriff auf das Objekt und versucht, es zu desinfizieren. Wenn das Objekt desinfiziert werden konnte, wird es zur Arbeit freigegeben. Wenn der Desinfektionsversuch erfolglos war, wird es gelöscht. Dabei wird eine Kopie des Objekts im Backup gespeichert. Ein Objekt mit dem Status *möglicherweise infiziert* wird in die Quarantäne verschoben.

[2] Wenn The Bat! als Mailprogramm verwendet wird, werden bei dieser Aktion gefährliche E-Mail-Objekte entweder desinfiziert oder gelöscht (abhängig davon, welche Aktion in The Bat! gewählt wurde).

Gewählte Aktion	**Was geschieht beim Fund eines gefährlichen Objekts?**
Zugriff verweigern **Desinfizieren** **Löschen**	Beim Fund eines infizierten oder möglicherweise infizierten Objekts löscht Mail-Anti-Virus das Objekt, ohne den Benutzer vorher zu benachrichtigen.

Bevor ein Desinfektionsversuch erfolgt oder das Objekt gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an und speichert diese im Backup (s. Pkt. 17.2 auf S. 262). Dadurch wird ermöglicht, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

KAPITEL 9. WEB-SCHUTZ

Bei der Arbeit im Internet besteht für die Informationen, die auf Ihrem Computer gespeichert sind, ständig das Risiko einer Infektion durch gefährliche Programme. Sie können in den Computer eindringen, während Sie im Internet bestimmte Seiten besuchen.

Um die Sicherheit Ihrer Arbeit im Internet zu garantieren, enthält Kaspersky Internet Security eine spezielle Komponente: *Web-Anti-Virus*. Er schützt Informationen, die über das HTTP-Protokoll auf Ihren Computer gelangen, und verhindert den Start gefährlicher Skripte auf Ihrem Computer.

> Achtung!
>
> Der Web-Schutz sieht die Kontrolle des HTTP-Datenverkehrs vor, der nur über die Ports, die in der Liste zu kontrollierenden Ports (s. Pkt. 17.7 auf S. 287) angegeben sind, vor. Eine Liste der Ports, die am häufigsten zur Übertragung von E-Mails und HTTP-Datenverkehr benutzt werden, ist im Lieferumfang des Programms enthalten. Wenn Sie Ports verwenden, die nicht zu dieser Liste gehören, sollten diese der Liste hinzugefügt werden, um den Schutz des über sie abgewickelten Datenverkehrs zu gewährleisten.

Wenn Sie in einer ungeschützten Umgebung arbeiten und die Internetverbindung mit Hilfe eines Modems erfolgt, ist es empfehlenswert, Web-Anti-Virus zum Schutz Ihrer Arbeit im Internet zu verwenden. Wenn Ihr Computer in einem Netzwerk arbeitet, das durch eine Firewall oder durch Filter für den HTTP-Verkehr geschützt ist, gewährleistet Web-Anti-Virus zusätzlichen Schutz bei der Arbeit im Internet.

Als Indikator für die Arbeit der Komponente dient das Symbol von Kaspersky Internet Security im Infobereich der Taskleiste, das jedes Mal bei der Untersuchung von Skripten folgendes Aussehen annimmt: .

Im Folgenden wird das Funktionsschema der Komponente näher beschrieben.

Web-Anti-Virus besteht aus zwei Modulen mit folgenden Funktionen:

- *Schutz des HTTP-Verkehrs* – Untersuchung aller Objekte, die über HTTP-Protokoll auf dem Computer eintreffen.
- *Skriptuntersuchung* – Untersuchung aller Skripts, die in Microsoft Internet Explorer bearbeitet werden, sowie aller WSH-Skripts (JavaScript, Visual Basic Script u.a.), die bei der Arbeit des Benutzers auf dem Computer und im Internet gestartet werden sollen.

Für das Programm Microsoft Internet Explorer ist ein spezielles Erweiterungsmodul vorgesehen, das bei der Installation von Kaspersky Internet Security in das Programm integriert wird. Es erlaubt die Ansicht einer Statistik über die von Web-Anti-Virus gesperrten gefährlichen Skripte. Über sein Vorhandensein informiert die Schaltfläche in der Symbolleiste des Browsers. Durch Klick auf diese Schaltfläche wird eine Infoleiste mit einer Statistik für Web-Anti-Virus geöffnet, welche die Anzahl der untersuchten und blockierten Skripts anzeigt.

Der Schutz des HTTP-Verkehrs erfolgt nach folgendem Algorithmus:

1. Jede Webseite oder Datei, auf die der Benutzer oder ein bestimmtes Programm über das Protokoll HTTP zugreift, wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert. Die Suche nach schädlichen Objekten erfolgt auf Basis der *Bedrohungssignaturen*, die bei der Arbeit von Kaspersky Internet Security verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus. Die Signaturen enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und Methoden zu deren Desinfektion. Der heuristische Algorithmus erlaubt es, neue Viren zu erkennen, die noch nicht in den Bedrohungssignaturen beschrieben sind.

2. Aufgrund der Virenuntersuchung bestehen folgende Varianten für das weitere Vorgehen:

   a. Wenn eine Webseite oder ein Objekt, auf das der Benutzer zugreift, schädlichen Code enthält, wird der Zugriff blockiert. Dabei erscheint auf dem Bildschirm eine Meldung darüber, dass das angeforderte Objekt oder die Seite infiziert ist.

   b. Wenn eine Datei oder eine Webseite keinen schädlichen Code enthält, erhält der Benutzer sofort Zugriff darauf.

Die Untersuchung von Skripten wird nach folgendem Algorithmus ausgeführt:

1. Jedes auf einer Webseite auszuführende Skript wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert.

2. Wenn das Skript schädlichen Code enthält, sperrt Web-Anti-Virus es und benachrichtigt den Benutzer durch eine spezielle Popup-Meldung.

3. Wenn im Skript kein schädlicher Code gefunden wird, wird es ausgeführt.

9.1. Auswahl der Web-Schutzstufe

Kaspersky Internet Security bietet die Sicherheit Ihrer Arbeit im Internet auf einer der folgenden Stufen (s. Abb. 29):

Hoch – Auf dieser Stufe erfolgt die Kontrolle von Skripten und Objekten, die über HTTP-Protokoll eintreffen, mit maximaler Ausführlichkeit. Das Programm untersucht ausführlich alle Objekte und verwendet dabei die vollständige Auswahl der Bedrohungssignaturen. Die Verwendung dieser Stufe wird in einer aggressiven Umgebung empfohlen, wenn keine anderen Mittel zum Schutz des HTTP-Verkehrs benutzt werden.

Empfohlen. Die Parameter dieser Stufe entsprechen den von Kaspersky Lab empfohlenen Einstellungen. Sie umfassen die Untersuchung der gleichen Objekte wie auf der Stufe **Hoch**. Allerdings ist die Zeit für die Zwischenspeicherung eines Dateifragments begrenzt, was erlaubt, die Untersuchung und Weiterleitung des Objekts an den Benutzer zu beschleunigen.

Niedrig – Diese Sicherheitsstufe erlaubt Ihnen, bequem mit Anwendungen, die den Arbeitsspeicher stark beanspruchen, zu arbeiten, weil die Auswahl der untersuchten Objekte auf dieser Stufe aufgrund der Verwendung einer beschränkten Auswahl von Bedrohungssignaturen eingeschränkt wird. Es wird empfohlen, diese Sicherheitsstufe zu wählen, wenn auf dem Computer zusätzliche Mittel zum Web-Schutz installiert sind.

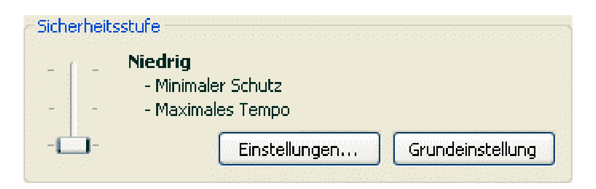


Abbildung 29. Auswahl der Sicherheitsstufe für Web-Anti-Virus

Der Web-Schutz erfolgt standardmäßig auf der **Empfohlenen** Stufe.

Sie können die Schutzstufe für Ihre Arbeit im Internet erhöhen oder senken, indem Sie die entsprechende Stufe wählen oder die Einstellungen der aktuellen Stufe ändern.

Um die Sicherheitsstufe zu ändern,

verschieben Sie den Zeiger auf der Skala. Durch das Anpassen der Schutzstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Objekte bestimmt: Je weniger Objekte der Analyse auf schädlichen Code unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn eine vordefinierte Stufe nicht Ihren Anforderungen entspricht, können Sie eine **Benutzerdefinierte** Sicherheitsstufe konfigurieren. Betrachten wir ein Beispiel, in dem diese nützlich sein kann.

Beispiel:

Ihr Computer wird über ein Modem mit dem Internet verbunden. Er ist nicht Teil eines lokalen Firmennetzwerks und ein Virenschutz des eingehenden HTTP-Verkehrs ist nicht vorhanden.

Bedingt durch die Besonderheiten Ihrer Arbeit laden Sie häufig große Dateien aus dem Internet herunter. In der Regel benötigt die Untersuchung solcher Dateien relativ viel Zeit.

Wie können Sie Ihren Computer optimal vor einer Infektion über den HTTP-Verkehr oder Skripte schützen?

Empfehlung zur Auswahl der Stufe:

Die Analyse der Situation lässt den Schluss zu, dass Ihr Computer in einer aggressiven Umgebung arbeitet und die Infektionsgefahr durch ein Schadprogramm über den HTTP-Verkehr sehr groß ist (Fehlen eines zentralen Web-Schutzes und Verbindungsmethode zum Internet).

Es wird empfohlen, von der vordefinierten Sicherheitsstufe **Hoch** auszugehen und diese folgendermaßen anzupassen: Die Zeitbegrenzung für die Zwischenspeicherung von Dateifragmenten bei der Untersuchung wird angepasst.

Um die Einstellungen einer vordefinierten Sicherheitsstufe anzupassen,

klicken Sie im Konfigurationsfenster für Web-Anti-Virus auf die Schaltfläche **Einstellungen**, passen Sie im folgenden Fenster die Parameter des Web-Schutzes an (s. Pkt. 9.2 auf S. 127) und klicken Sie auf **OK**.

9.2. Konfiguration des Web-Schutzes

Der Web-Schutz garantiert die Untersuchung aller Objekte, die mit dem HTTP-Protokoll auf Ihren Computer heruntergeladen werden, und bietet die Kontrolle über alle WSH-Skripts (JavaScript, Visual Basic Script u.a.), die gestartet werden sollen.

Sie können folgende Parameter für Web-Anti-Virus anpassen, welche der beschleunigten Arbeit der Komponente dienen:

- Sie können den Untersuchungsalgorithmus festlegen, indem Sie die Verwendung der vollständigen oder einer begrenzten Auswahl der Bedrohungssignaturen wählen.
- Sie können eine Liste der Adressen anlegen, deren Inhalt Sie vertrauen.

Außerdem können Sie die Aktion für gefährliche Objekte im HTTP-Verkehr wählen, die von Web-Anti-Virus damit ausgeführt werden soll.

In diesem Abschnitt des Handbuchs werden alle oben genannten Parameter ausführlich beschrieben.

9.2.1. Festlegen des Untersuchungsalgorithmus

Die Untersuchung der Daten, die aus dem Internet empfangen werden, kann nach einem der folgenden Algorithmen erfolgen:

- *Quick-Scan* – Technologie zum Erkennen von schädlichem Code im Netzwerkverkehr, bei welcher der Datenstrom "on the fly" untersucht wird. Wenn Sie beispielsweise eine Datei aus dem Internet herunterladen, untersucht Web-Anti-Virus die Datei in den Portionen, in denen die Daten auf den Computer kopiert werden. Diese Technologie erlaubt eine erhöhte Zustellungsgeschwindigkeit des untersuchten Objekts an den Benutzer. Gleichzeitig wird zur Realisierung der schnellen Untersuchung die Auswahl der Bedrohungssignaturen eingeschränkt (nur die aktivsten Bedrohungen), wodurch das Sicherheitsniveau Ihrer Arbeit im Internet wesentlich sinkt.

- *Mit Zwischenspeicherung untersuchen* – Technologie zum Erkennen von schädlichem Code im Netzwerkverkehr, bei welcher die Untersuchung eines Objekts erfolgt, nachdem es vollständig in den Zwischenspeicher kopiert wurde. Danach wird dieses Objekt der Virenanalyse unterzogen und in Abhängigkeit von den Analyseergebnissen dem Benutzer zur Arbeit übergeben oder blockiert.

  Bei der Verwendung dieses Untersuchungstyps werden die vollständigen Bedrohungssignaturen verwendet, wodurch die Sicherheit vor schädlichem Code erheblich gesteigert wird. Allerdings erhöht die Verwendung dieses Algorithmus die Zeit für die Objektuntersuchung und für dessen Freigabe an den Benutzer. Außerdem können beim Kopieren und bei der Bearbeitung großer Objekte Probleme auftreten, die mit einer Zeitüberschreitung bei der Verbindung mit dem HTTP-Client zusammenhängen.

  Um dieses Problem zu lösen, empfehlen wir, die Zeit für die Zwischenspeicherung von Fragmenten eines aus dem Internet empfangenden Objekts zu beschränken. Bei Überschreiten des Zeitlimits wird jeder heruntergeladene Teil der Dateien ungeprüft dem Benutzer übergeben. Nach dem Abschluss des Downloads wird das Objekt vollständig untersucht. Dadurch lässt sich die Dauer für die Übertragung des Objekts an den Benutzer verringern und das Problem einer Verbindungsstörung lösen, ohne das Sicherheitsniveau bei der Arbeit im Internet einzuschränken.

Zur Auswahl des Untersuchungsalgorithmus, den Web-Anti-Virus verwenden soll:

1. Klicken Sie im Konfigurationsfenster von Web-Anti-Virus auf die Schaltfläche **Einstellungen**.
2. Wählen Sie im folgenden Fenster (s. Abb. 30) den gewünschten Wert im Block **Untersuchungsalgorithmus**.

In der Grundeinstellung untersucht Web-Anti-Virus die Daten aus dem Internet mit Zwischenspeicherung und verwendet die vollständigen Bedrohungssignaturen. Außerdem beträgt das Zeitlimit für die Zwischenspeicherung von Dateifragmenten 1 Sekunde.

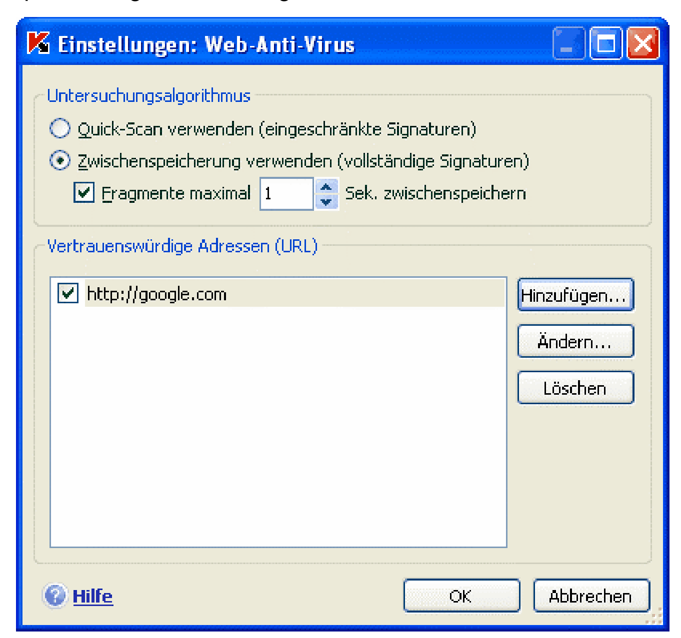


Abbildung 30. Einstellungen der Web-Schutzstufe

Achtung!

Wenn es während der Arbeit mit Ressourcen wie Internet-Radio, Internet-Video und Internet-Konferenzen zu Problemen beim Zugriff auf angeforderte Objekte kommt, verwenden Sie den Algorithmus Quick-Scan.

9.2.2. Erstellen einer Liste der vertrauenswürdigen Adressen

Ihnen wird die Möglichkeit geboten, eine Liste der vertrauenswürdigen Adressen anzulegen, deren Inhalt Sie vorbehaltlos vertrauen. Web-Anti-Virus wird die Informationen von diesen Adressen nicht auf gefährliche Objekte hin analysieren. Diese Option kann benutzt werden, wenn Web-Anti-Virus das Laden einer bestimmten Datei verhindert, indem er den Downloadversuch blockiert.

Um eine Liste mit vertrauenswürdigen Adressen anzulegen,

1. Klicken Sie im Konfigurationsfenster von Web-Anti-Virus auf die Schaltfläche **Einstellungen**.
2. Erstellen Sie im folgenden Fenster (s. Abb. 30) die Liste der vertrauenswürdigen Server im Block **Vertrauenswürdige Adressen (URL)**. Verwenden Sie dazu die rechts angebrachten Schaltflächen.

Bei der Angabe einer vertrauenswürdigen Adresse können Sie Masken benutzen, die folgende Sonderzeichen enthalten:

***** – beliebige Zeichenfolge.
Beispiel: Wird die Maske ***abc*** angegeben, dann wird eine beliebige URL-Adresse, in der die Zeichenfolge **abc** enthalten ist, nicht untersucht. Beispiel: www.virus.com/download_virus/page_0-9abcdef.html.

? – ein beliebiges Zeichen.
Beispiel: Bei Angabe der Maske **Patch_123?.com** wird eine URL-Adresse nicht untersucht, die diese Zeichenfolge und ein beliebiges Zeichen enthält, das auf die 3 folgt, beispielsweise **Patch_1234.com**. Die Adresse **patch_12345.com** wird dagegen untersucht.

Wenn die Zeichen ***** und **?** Bestandteil einer realen URL-Adresse sind, die der Liste hinzugefügt werden soll, dann muss bei der Angabe das Zeichen **** benutzt werden, damit eines der Zeichen *****, **?**, **** nicht als Platzhalter interpretiert wird.

Beispiel: Folgende URL-Adresse soll als vertrauenswürdige Adresse festgelegt werden: www.virus.com/download_virus/virus.dll?virus_name=

Damit Kaspersky Internet Security das Zeichen **?** nicht als Zeichen für eine Ausnahme interpretiert, muss dem **?** das Zeichen **** vorangestellt werden. In diesem Fall muss die URL-Adresse also in folgender Form zur Liste der Ausnahmen hinzugefügt werden:
www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Wiederherstellen der Standardparameter für den Web-Schutz

Während Sie die Arbeit von Web-Anti-Virus anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Parameter für Web-Anti-Virus wiederherzustellen,

1. Wählen Sie die Komponente **Web-Anti-Virus** im Hauptfenster aus und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Komponente.
2. Klicken Sie im Abschnitt **Sicherheitsstufe** auf die Schaltfläche **Grundeinstellung**.

9.2.4. Auswahl der Aktion für ein gefährliches Objekt

Wenn sich durch die Analyse eines Objekts des HTTP-Verkehrs herausstellt, dass das Objekt schädlichen Code enthält, sind die weiteren Operationen von Web-Anti-Virus von der Aktion abhängig, die Sie festgelegt haben.

Um die Reaktion von Web-Anti-Virus beim Fund eines gefährlichen Objekts zu bestimmen:

öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security und wählen Sie die Komponente **Web-Anti-Virus**. Alle verfügbaren Aktionen für gefährliche Objekte sind im Block **Aktion** angegeben (s. Abb. 31).

Standardmäßig zeigt Web-Anti-Virus beim Fund eines gefährlichen Objekts im HTTP-Verkehr auf dem Bildschirm eine Warnung an und bietet mehrere Aktionen für das Objekt zur Auswahl an.



Abbildung 31. Auswahl der Aktion für ein gefährliches Skript

Betrachten wir die möglichen Varianten zur Bearbeitung gefährlicher Objekte des HTTP-Verkehrs genauer.

Gewählte Aktion	**Was geschieht beim Fund eines gefährlichen Objekts im HTTP-Verkehr?**
Aktion erfragen	Web-Anti-Virus zeigt eine Warnmeldung auf dem Bildschirm an, die darüber informiert, von welchem schädlichen Code das Objekt infiziert ist, und bietet Aktionen zur Auswahl an.
Blockieren	Web-Anti-Virus sperrt den Zugriff auf das Objekt und zeigt eine Meldung über das Blockieren auf dem Bildschirm an. Informationen darüber werden im Bericht aufgezeichnet (s. Pkt. 17.3 auf S. 265).
Erlauben	Web-Anti-Virus erlaubt den Zugriff auf das Objekt. Informationen darüber werden im Bericht aufgezeichnet.

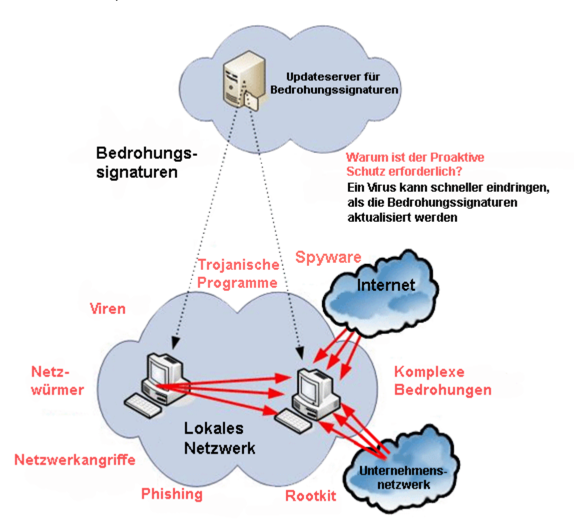
Web-Anti-Virus sperrt die Ausführung gefährlicher Skripte und zeigt auf dem Bildschirm eine Popup-Meldung an, die den Benutzer über die ausgeführte Aktion informiert. Die Aktion für ein gefährliches Skript kann nicht vom Benutzer geändert werden. Es besteht höchstens die Möglichkeit, die Arbeit des Moduls zur Skriptuntersuchung zu deaktivieren.

KAPITEL 10. PROAKTIVER SCHUTZ FÜR IHREN COMPUTER

Achtung!

Für Computer mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition sowie für Computer, auf denen das Betriebssystem Microsoft Windows Vista oder Microsoft Windows Vista x64 installiert ist, sind in dieser Version der Anwendung folgende Komponenten des Proaktiven Schutzes nicht verfügbar: **Integritätskontrolle für Anwendungen** und **Untersuchung von VBA-Makros**.

Kaspersky Internet Security schützt nicht nur vor bekannten, sondern auch vor neuen Bedrohungen, über die noch keine Informationen in die Datenbanken mit den Bedrohungssignaturen aufgenommen wurden. Dafür wurde eine spezielle Komponente entwickelt, der *Proaktive Schutz*.



Der Proaktive Schutz wurde notwendig, nachdem sich Schadprogramme schneller ausbreiten, als der Virenschutz durch Updates, die zur Neutralisierung dieser Bedrohungen fähig sind, aktualisiert werden kann. Die reaktiven

Technologien, auf denen der Virenschutz beruht, erfordern mindestens eine tatsächliche Infektion durch eine neue Bedrohung sowie eine bestimmte Zeit, um den schädlichen Code zu analysieren, die neuen Informationen zu den Datenbanken mit den Bedrohungssignaturen hinzuzufügen und diese Datenbank auf den Benutzercomputern zu aktualisieren. Während dieser Zeit kann eine neue Bedrohung bereits gewaltigen Schaden verursachen.

Durch die präventiven Technologien, auf denen der Proaktive Schutz von Kaspersky Internet Security basiert, lässt sich ein solcher Zeitverlust vermeiden und eine neue Bedrohung neutralisieren, noch bevor sie auf Ihrem Computer Schaden verursachen kann. Wie wird das erreicht? Im Unterschied zu den reaktiven Technologien, bei denen die Analyse auf der Basis von Einträgen der Datenbank für die Bedrohungssignaturen erfolgt, erkennen die Präventivtechnologien eine neue Bedrohung auf Ihrem Computer an der Reihenfolge der Aktionen, die von einem bestimmten Programm ausgeführt werden sollen. Zum Lieferumfang der Anwendung gehört eine Sammlung von Kriterien, mit deren Hilfe sich bestimmen lässt, wie gefährlich die Aktivität eines bestimmten Programms ist. Wenn die Aktionsreihenfolge eines bestimmten Programms aufgrund der Aktivitätsanalyse einen Verdacht ergibt, wendet Kaspersky Internet Security die Aktion an, die in der Regel für eine Aktivität solcher Art festgelegt ist.

Eine gefährliche Aktivität wird durch die Gesamtheit der Programmaktionen charakterisiert. Wenn sich ein bestimmtes Programm beispielsweise selbst in Netzwerkressourcen, in den Autostart-Ordner oder in die Systemregistrierung kopiert und anschließend Kopien verschickt, besteht eine hohe Wahrscheinlichkeit, dass es sich bei diesem Programm um einen Wurm handelt. Als gefährliche Aktivitäten gelten auch:

- Veränderungen des Dateisystems
- Einfügen von Modulen in andere Prozesse
- versteckte Prozesse im System
- Veränderung von bestimmten Schlüsseln der Microsoft Windows-Systemregistrierung

Alle gefährlichen Operationen werden vom Proaktiven Schutz verfolgt und blockiert. Der Proaktive Schutz überwacht auch die Ausführung aller Makros, die in Microsoft Office-Anwendungen gestartet werden sollen.

Bei seiner Arbeit verwendet der Proaktive Schutz eine Auswahl von im Lieferumfang der Anwendung enthaltenen Regeln sowie Regeln, die der Benutzer bei der Arbeit mit der Anwendung erstellt. Eine *Regel* ist eine Kombination von Kriterien, welche die Gesamtheit verdächtiger Aktionen und die Reaktion von Kaspersky Internet Security auf diese Aktionen festlegen.

Es sind separate Regeln für die Aktivität von Anwendungen, für die Kontrolle von Veränderungen der Systemregistrierung und für auf dem Computer gestartete

Makros und Programme vorhanden. Sie können die Regeln nach eigenem Ermessen anpassen, Regeln hinzufügen, löschen oder ändern. Es gibt Erlaubnis- und Verbotsregeln.

Der Proaktive Schutz funktioniert nach folgendem Algorithmus:

1. Der Proaktive Schutz analysiert sofort nach dem Start des Computers die folgenden Aspekte:

    - *Aktionen jeder Anwendung, die auf dem Computer gestartet wird*. Der Verlauf der ausgeführten Aktionen und ihre Reihenfolge werden gespeichert und mit der Reihenfolge verglichen, die für eine gefährliche Aktivität charakteristisch ist (Im Lieferumfang des Programms ist eine Datenbank der Arten von gefährlichen Aktivitäten enthalten, die zusammen mit den Bedrohungssignaturen aktualisiert wird).

    - *Aktionen jedes VBA-Makros, das gestartet werden soll*. Das Makro wird auf das Vorhandensein von Merkmalen geprüft, die für schädliche Aktivität charakteristisch sind.

    - *Integrität der Programm-Module*, der auf Ihrem Computer installierten Anwendungen. Dadurch kann die Veränderung von Anwendungsmodulen und das Einfügen von schädlichem Code in Module verhindert werden.

    - *Jeder Versuch zur Veränderung der Systemregistrierung* (Löschen oder Hinzufügen eines Systemregistrierungsschlüssels, Eingabe von Schlüsselwerten in einem ungültigen Format, das Ansicht und Ändern der Schlüssel verhindert, usw.).

2. Die Analyse erfolgt auf der Basis der Erlaubnis- und Verbotsregeln des Proaktiven Schutzes.

3. Als Ergebnis der Analyse sind folgende Varianten für das weitere Vorgehen möglich:

    - Wenn eine Aktivität die Bedingungen einer Erlaubnisregel des Proaktiven Schutzes erfüllt oder nicht unter eine Verbotsregel fällt, wird sie nicht blockiert.

    - Wenn eine Aktivität in einer Verbotsregel beschrieben ist, erfolgt das weitere Vorgehen der Komponente in Übereinstimmung mit der in der Regel festgelegten Aktionsreihenfolge. Gewöhnlich wird eine solche Aktivität blockiert. Auf dem Bildschirm erscheint ein Hinweis, in dem die Anwendung, der Typ ihrer Aktivität und der Verlauf der ausgeführten Aktionen angegeben werden. Sie müssen selbständig eine Entscheidung über Erlaubnis oder Verbot für

diese Aktivität fällen. Sie können eine Regel für die Aktivität erstellen und die im System ausgeführten Aktionen rückgängig machen.

10.1. Konfiguration des Proaktiven Schutzes

Der Proaktive Schutz erfolgt genau nach den Parametern (s. Abb. 32), die festlegen:

- *ob die Aktivität der Anwendungen auf Ihrem Computer kontrolliert wird.*

  Dieser Modus des Proaktiven Schutzes wird durch das Kontrollkästchen ☑ **Aktivitätsanalyse aktivieren** geregelt. Der Modus ist standardmäßig aktiviert, wodurch die strenge Kontrolle über die Aktionen jedes Programms gewährleistet wird, das auf Ihrem Computer gestartet werden soll. Für bestimmte Arten gefährlicher Aktivität können Sie die Art der Bearbeitung von Anwendungen (s. Pkt. 10.1.1 auf S. 138) mit der betreffenden Aktivität festlegen. Außerdem besteht die Möglichkeit, Ausnahmen für den Proaktiven Schutz festzulegen, wodurch die Aktivität der ausgewählten Anwendungen von der Kontrolle ausgeschlossen wird.

- *ob die Kontrolle der Integrität von Anwendungen aktiviert ist.*

  Diese Funktionalität ist verantwortlich für die Integrität von Modulen der auf Ihrem Computer installierten Anwendungen und wird durch das Kontrollkästchen ☑ **Integritätskontrolle aktivieren** reguliert. Die Integrität wird anhand des Bestands der Module eines Programms und der Kontrollsumme des Abbilds des eigentlichen Programms überwacht. Sie können Regeln für die Kontrolle der Integrität von Modulen einer bestimmten Anwendung erstellen. Dazu muss die betreffende Anwendung in die Liste der zu kontrollierenden Anwendungen aufgenommen werden.

  > Diese Komponente des Proaktiven Schutzes ist nicht in der Anwendung vorhanden, wenn sie auf einem Computer mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64 installiert ist.

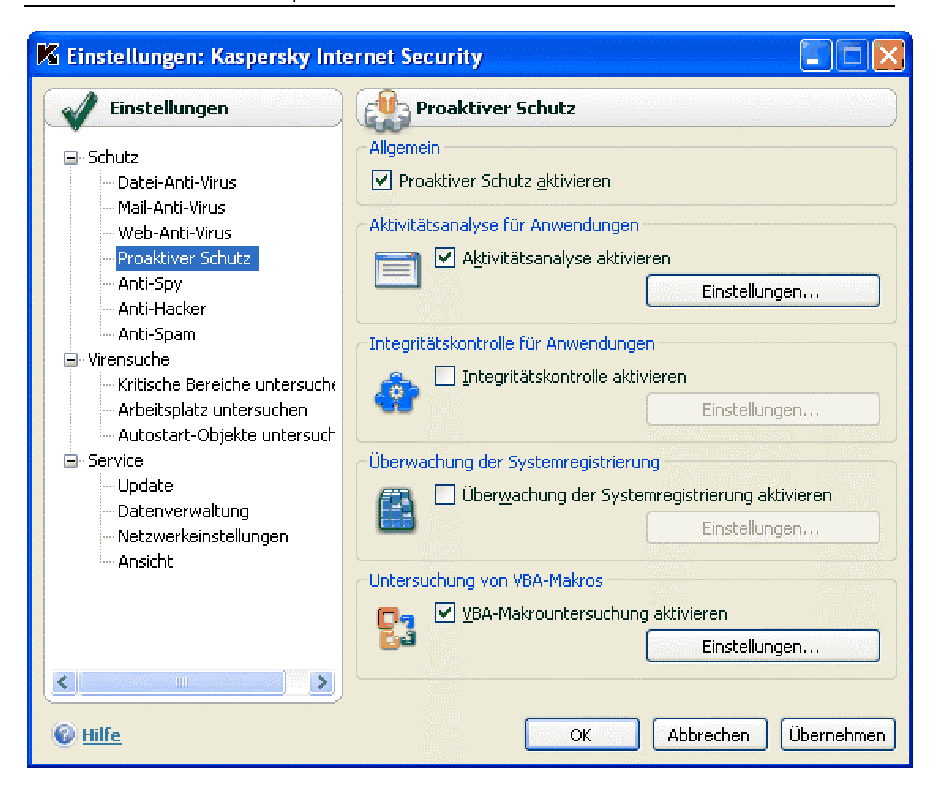


Abbildung 32. Einstellungen für den Proaktiven Schutz

- *ob die Kontrolle über Veränderungen der Systemregistrierung erfolgt.*

  Das Kontrollkästchen ☑ **Überwachung der Systemregistrierung aktivieren** ist standardmäßig aktiviert, was bedeutet, dass Kaspersky Internet Security jeden Versuch zur Veränderung eines der Kontrolle unterliegenden Schlüssels in der Systemregistrierung des Betriebssystems Microsoft Windows analysiert.

  Sie können eigene Regeln (s. Pkt. 10.1.4.2 auf S. 153) zur Kontrolle eines bestimmten Registrierungsschlüssels erstellen.

- *ob die Makrountersuchung ausgeführt wird.*

  Die Kontrolle über die Makroausführung auf Ihrem Computer wird durch das Kontrollkästchen ☑ **VBA-Makrountersuchung aktivieren** reguliert. Das Kontrollkästchen ist standardmäßig aktiviert, was bedeutet, dass alle Aktionen von Visual Basic for Applications-Makros der Kontrolle des Proaktiven Schutzes unterliegen.

Sie können auswählen, welche Makros als gefährlich gelten und wie sie behandelt werden sollen (s. Pkt. 10.1.3 auf S. 147).

> Diese Komponente des Proaktiven Schutzes ist nicht in der Anwendung vorhanden, wenn sie auf einem Computer mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista und Microsoft Windows Vista x64 installiert ist.

Sie können Ausnahmen für die Module des Proaktiven Schutzes festlegen (s. Pkt. 6.3.1 auf S. 80) und eine Liste der vertrauenswürdigen Anwendungen (s. Pkt. 6.3.2 auf S. 85) erstellen.

Im folgenden Abschnitt des Handbuchs werden alle oben genannten Aspekte ausführlich beschrieben.

10.1.1. Regeln für die Aktivitätskontrolle

> Beachten Sie, dass die Einstellungen für die Aktivitätskontrolle in der Anwendung unterschiedlich sind, je nachdem, ob die Anwendung auf einem Computer mit einem der Betriebssysteme Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64 installiert ist oder auf einem Computer mit anderen Betriebssystemen.
>
> Informationen über die Einstellungen für die Aktivitätskontrolle für die genannten Betriebssysteme finden Sie am Ende dieses Abschnitts.

Die Aktivität der Anwendungen auf Ihrem Computer wird von Kaspersky Internet Security kontrolliert. Zum Lieferumfang der Anwendung gehört eine Liste mit Beschreibungen von Ereignissen, die als gefährlich gelten können. Für jedes dieser Ereignisse existiert eine Regel. Wenn die Aktivität einer bestimmten Anwendung als gefährliches Ereignis eingestuft wird, folgt der Proaktive Schutz den Anweisungen, die in der Regel für dieses Ereignis festgelegt sind.

Kreuzen Sie das Kontrollkästchen ☑ **Aktivitätsanalyse aktivieren** an, damit die Aktivität der Anwendungen kontrolliert wird.

Im Folgenden werden einige Arten von Ereignissen beschrieben, die im System eintreten können und von der Anwendung als verdächtig behandelt werden:

- *Gefährliche Aktivität (Verhaltensanalyse)*. Kaspersky Internet Security analysiert die Aktivität der Anwendungen, die auf dem Computer installiert sind, und erkennt auf Basis einer Regelliste, die von den Kaspersky-Lab-Spezialisten angelegt wurde, gefährliche und verdächtige Aktionen der Anwendungen. Als solche Aktionen gelten beispielsweise die versteckte Installation eines Programms und das von einem Programm selbst ausgeführte Kopieren.

- *Browserstart mit Parametern*. Die Analyse dieses Aktivitätstyps erlaubt es, Versuche zum versteckten Start eines Browsers mit Parametern zu erkennen. Diese Aktivität ist charakteristisch für den Start eines Webbrowsers aus einer Anwendung mit bestimmten Befehlszeilenschlüsseln: z.B. bei der Verwendung von in einem Werbebrief Ihrer Mailbox enthaltenen Links zu einer bestimmten Adresse im Internet.

- *Eindringen in Prozess*. Hinzufügen von ausführbarem Code zum Prozess eines bestimmten Programms oder Erstellen eines zusätzlichen Datenstroms. Diese Aktivität ist charakteristisch für trojanische Programme.

- *Auftreten eines versteckten Prozesses (Rootkit)*. Ein Rootkit ist eine Auswahl von Programmen, die benutzt werden, um schädliche Programme und ihre Prozesse im System zu tarnen. Kaspersky Internet Security analysiert das Betriebssystem auf das Vorhandensein versteckter Prozesse.

- *Eindringen von Fenster-Hooks*. Diese Aktivität wird beim Versuch zum Lesen von Kennwörtern und anderen geheimen Informationen, die in Dialogfenstern des Betriebssystems angezeigt werden, verwendet. Kaspersky Internet Security überwacht diese Aktivität beim Versuch des Abfangens von Informationen, die zwischen Betriebssystem und Dialogfenstern ausgetauscht werden.

- *Verdächtige Werte in der Registrierung*. Die Systemregistrierung ist eine Datenbank, in der die System- und Benutzereinstellungen gespeichert sind, welche die Arbeit des Betriebssystems Microsoft Windows sowie der auf dem Computer installierten Dienste regulieren. Schädliche Programme verändern bestimmte Werte in den Registrierungsschlüsseln und versuchen dadurch die eigene Existenz im System zu verheimlichen. Kaspersky Internet Security analysiert die Systemregistrierungseinträge auf das Vorhandensein verdächtiger Werte.

- *Verdächtige Aktivität im System*. Die Anwendung analysiert die Aktionen, die vom Betriebssystem Microsoft Windows ausgeführt werden, und erkennt verdächtige Aktivität. Ein Beispiel für verdächtige Aktivität ist eine Integritätsverletzung, die beispielsweise darin bestehen kann, dass ein oder mehrere Module einer kontrollierten Anwendung seit dem vorhergehenden Start verändert wurden.

- *Erkennen von Tastaturspionen*. Diese Aktivität wird von schädlichen Programmen benutzt, um über die Tastatur eingegebene Informationen abzufangen.

- *Schutz für Microsoft Windows-Task-Manager*. Kaspersky Internet Security schützt den Task-Manager vor dem Eindringen schädlicher Module, deren Aktivität darauf abzielt, die Arbeit des Managers zu blockieren.

Die Liste der gefährlichen Aktivitäten wird beim Update von Kaspersky Internet Security automatisch ergänzt und kann nicht verändert werden. Sie können:

- die Kontrolle einer bestimmten Aktivität ablehnen. Deaktivieren Sie dazu das Kontrollkästchen neben ihrem Namen.
- eine Regel ändern, nach welcher der Proaktive Schutz beim Fund einer gefährlichen Aktivität vorgeht.
- eine Liste von Ausnahmen erstellen (s. Pkt. 6.3 auf S. 79), indem Sie die Anwendungen festlegen, deren Aktivität Sie nicht für gefährlich halten.

Um zur Konfiguration der Aktivitätskontrolle zu wechseln,

1. Öffnen Sie mit dem Link Einstellungen im Programmhauptfenster das Konfigurationsfenster von Kaspersky Internet Security.
2. Wählen Sie in der Konfigurationsstruktur die Komponente **Proaktiver Schutz**.
3. Klicken Sie auf die Schaltfläche **Einstellungen** im Block **Aktivitätsanalyse für Anwendungen**.

Die Arten gefährlicher Aktivität, die vom Proaktiven Schutz kontrolliert werden, werden im Fenster **Einstellungen: Aktivitätsanalyse** genannt (s. Abb. 33).

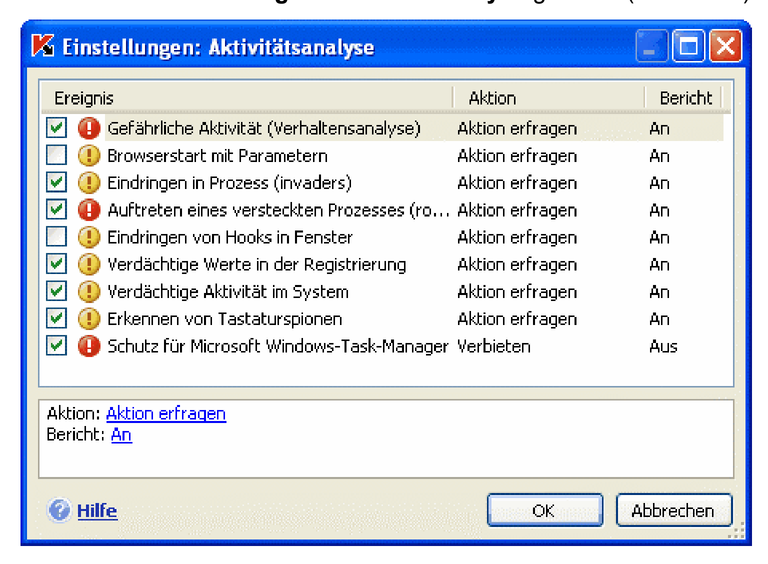


Abbildung 33. Einstellungen für die Aktivitätskontrolle von Anwendungen

Um eine Regel für die Kontrolle einer gefährlichen Aktivität anzupassen, wählen Sie diese in der Liste aus und legen Sie im unteren Bereich der Registerkarte die Parameter der Regel fest:

- Wählen Sie die Reaktion des Proaktiven Schutzes auf die gefährliche Aktivität.

  Als Reaktion kann eine der folgenden Aktionen dienen: Erlauben, Aktion erfragen oder Prozess beenden. Klicken Sie mit der linken Maustaste auf den Link mit der Aktion, bis er den gewünschten Wert annimmt. Zusätzlich zum Beenden eines Prozesses kann die Anwendung, die die gefährliche Aktivität initiiert hat, unter Quarantäne gestellt werden. Verwenden Sie dazu den Link An/Aus neben dem entsprechenden Parameter. Für die Suche nach versteckten Prozessen im System können Sie zusätzlich das Intervall angeben, in dem die Untersuchung gestartet werden soll.

- Geben Sie an, ob ein Bericht über die ausgeführte Operation erstellt werden soll. Verwenden Sie dazu den Link An/Aus.

Um die Kontrolle einer bestimmten gefährlichen Aktivität abzulehnen, deaktivieren Sie in der Liste der gefährlichen Aktivitäten das Kontrollkästchen ☑ neben seinem Namen.

Besonderheiten der Einstellungen für die Aktivitätsanalyse von Anwendungen in Kaspersky Internet Security unter den Betriebssystemen Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64:

Wenn der Computer unter einem der oben genannten Betriebssystem läuft, wird nur eine Art von Ereignissen kontrolliert, die im System eintreten können: gefährliche Aktivität (Verhaltensanalyse). Damit Kaspersky Internet Security zusätzlich auch Veränderungen von Systembenutzerkonten überwacht, aktivieren Sie das Kontrollkästchen ☑ **Systembenutzerkonten kontrollieren** (s. Abb. 34).

Benutzerkonten regulieren den Zugriff auf das System und definieren den Benutzer und seine Arbeitsumgebung. Dadurch werden Beschädigungen des Betriebssystems oder der Daten anderer Benutzer verhindert. Eine gefährliche Aktivität besteht im Verändern von Benutzerkonten (beispielsweise Ändern eines Kennworts).

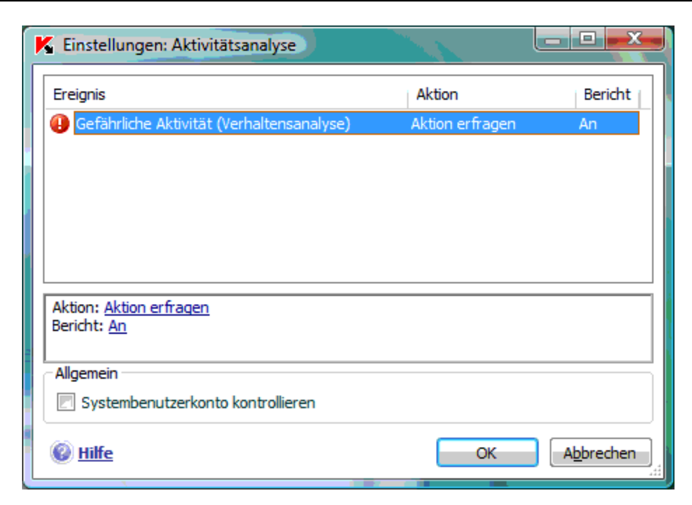


Abbildung 34. Einstellungen für die Aktivitätskontrolle von Anwendungen unter Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64

10.1.2. Integritätskontrolle für Anwendungen

Diese Komponente des Proaktiven Schutzes funktioniert nicht auf Computern mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64.

Es existiert eine Reihe von für das System kritischen Programmen, die von schädlichen Programmen zur Ausbreitung verwendet werden können. Dazu zählen beispielsweise Browser, Mailprogramme sowie Systemanwendungen und Prozesse, die zur Verbindung mit dem Internet und bei der Arbeit mit E-Mails und anderen Dokumenten verwendet werden. Deshalb gelten solche Anwendungen hinsichtlich der Aktivitätskontrolle als *kritisch*.

Der Proaktive Schutz kontrolliert kritische Anwendungen, analysiert ihre Aktivität, die Integrität des Modulbestands dieser Anwendungen und den Start anderer Prozesse durch diese Anwendungen. Im Lieferumfang von Kaspersky Internet Security ist eine Liste kritischer Anwendungen enthalten. Für jede kritische Anwendung existiert eine spezielle Kontrollregel, welche die Aktivität der Anwendung reguliert. Sie können die Liste durch andere Anwendungen, die Ihrer Meinung nach kritisch sind, ergänzen und Regeln für Anwendungen der mitgelieferten Liste löschen oder anpassen.

Neben der Liste kritischer Anwendungen ist auch eine Auswahl vertrauenswürdiger Module vorhanden, die in alle der Kontrolle unterliegenden Anwendungen geladen werden dürfen. Dazu zählen beispielsweise Module, die über eine Signatur der Microsoft Corporation verfügen. Die Aktivität von Anwendungen, zu denen diese Module gehören, ist mit hoher Wahrscheinlichkeit unschädlich, weshalb eine strenge Kontrolle über die Aktionen nicht erforderlich ist. Die Kaspersky-Lab-Spezialisten haben eine Liste dieser Module erstellt, um die Belastung Ihres Computers bei der Arbeit des Proaktiven Schutzes zu verringern.

In der Grundeinstellung werden Komponenten, die eine Signatur der Microsoft Corporation besitzen, automatisch zur Liste der vertrauenswürdigen Anwendungen hinzugefügt. Bei Bedarf können Komponenten zur Liste hinzugefügt oder daraus entfernt werden.

Die Kontrolle über Systemprozesse wird durch das Kontrollkästchen ☑ **Integritätskontrolle aktivieren** reguliert. Das Kontrollkästchen ist standardmäßig deaktiviert. Wenn die Integritätskontrolle aktiv ist, wird jede Anwendung bzw. Anwendungsmodul, die/das gestartet werden soll, auf Zugehörigkeit zur Liste der kritischen oder vertrauenswürdigen Anwendungen geprüft. Wenn eine Anwendung auf der Liste der kritischen Anwendungen steht, wird ihre Aktivität der Kontrolle durch den Proaktiven Schutz unterzogen, wozu die dafür erstellte Regel dient.

Um zur Konfiguration der Prozessüberwachung zu wechseln,

1. Öffnen Sie mit dem Link Einstellungen des Programmhauptfensters das Konfigurationsfenster von Kaspersky Internet Security.
2. Wählen Sie in der Konfigurationsstruktur die Komponente **Proaktiver Schutz**.
3. Klicken Sie im Block **Integritätskontrolle für Anwendungen** auf die Schaltfläche **Einstellungen**.

Im Folgenden wird die Arbeit mit kritischen und vertrauenswürdigen Prozessen genauer beschrieben.

10.1.2.1. Konfiguration von Kontrollregeln für kritische Anwendungen

Kritische Anwendungen sind ausführbare Programmdateien, deren Aktivitätskontrolle von hoher Bedeutung ist, weil solche Programme von schädlichen Objekten verwendet werden können, um sich selbst auszubreiten.

Eine Liste kritischer Anwendungen befindet sich auf der Registerkarte **Zu überwachende Anwendungen** (s. Abb. 35). Diese Liste wurde von den Kaspersky-Lab-Spezialisten erstellt und gehört zum Lieferumfang der

Anwendung. Für jede kritische Anwendung gibt es eine Kontrollregel, welche die Aktivität dieser Anwendung reguliert. Sie können die vorhandenen Regeln anpassen und eigene Regeln erstellen.

Der Proaktive Schutz analysiert folgende Operationen mit kritischen Anwendungen: Start, Ändern der Zusammensetzung von Anwendungsmodulen und Start einer Anwendung als untergeordneter Prozess. Für jede der genannten Operationen können Sie eine Reaktion des Proaktiven Schutzes wählen (Operation erlauben oder verbieten). Außerdem kann festgelegt werden, ob die Aktivität in einem Bericht über die Arbeit der Komponente festgehalten werden soll. Standardmäßig werden praktisch für alle kritischen Anwendungen die Operationen zum Starten, Ändern oder Starten von untergeordneten Prozessen erlaubt.

Um eine Anwendung zur Liste der kritischen Anwendungen hinzuzufügen und eine Regel dafür zu erstellen,

1. Klicken Sie auf der Registerkarte **Zu überwachende Anwendungen** auf die Schaltfläche **Hinzufügen**. Dadurch öffnet sich das Kontextmenü, in dem Sie mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl oder mit dem Punkt **Anwendungen** zur Liste der momentan laufenden Anwendungen gelangen, um die gewünschte Anwendung auszuwählen. Die Anwendung wird der Liste an erste Stelle hinzugefügt. Standardmäßig wird eine Erlaubnisregel für sie erstellt. Beim ersten Start dieser Anwendung wird eine Liste der während des Starts benutzten Module angelegt. Diese Module werden erlaubt.

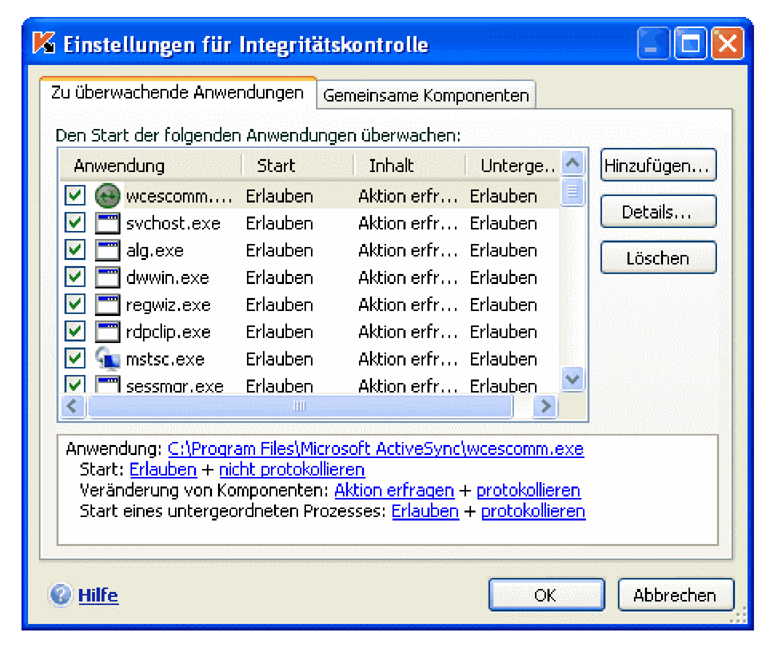


Abbildung 35. Einstellungen für die Integritätskontrolle für Anwendungen

2. Markieren Sie die Regel in der Liste und legen Sie im unteren Bereich der Registerkarte die Parameter der Regel fest:

   - Bestimmen Sie, wie der Proaktive Schutz reagieren soll, wenn versucht wird, die kritische Anwendung zu starten, ihre Module zu verändern oder eine kritische Anwendung als untergeordneten Prozess zu starten.

     Als Reaktion stehen folgende Aktionen zur Auswahl: erlauben, Aktion erfragen und verbieten. Klicken Sie mit der linken Maustaste auf den Link mit der Aktion, bis er den gewünschten Wert annimmt.

   - Legen Sie fest, ob ein Bericht über die ausgeführte Operation erstellt werden soll. Verwenden Sie dazu den Link protokollieren/nicht protokollieren.

Um die Kontrolle über die Aktivität einer bestimmten Anwendung abzulehnen, deaktivieren Sie neben ihrem Namen das Kontrollkästchen ☑.

Verwenden Sie die Schaltfläche **Details**, um Details für die Liste der Module der gewählten Anwendung anzuzeigen. Das folgende Fenster **Einstellungen: Anwendungsmodule** enthält eine Liste der Module, die zur zu kontrollierenden

Anwendung gehören und bei ihrem Start verwendet werden. Sie können die Liste mit Hilfe der Schaltflächen **Hinzufügen** und **Löschen** bearbeiten. Die Schaltflächen befinden sich auf der rechten Seite des Fensters.

Außerdem können Sie erlauben oder verbieten, dass ein bestimmtes Modul von der zu kontrollierenden Anwendung geladen wird. Standardmäßig wird für jedes Modul eine Erlaubnisregel erstellt. Um die Aktion zu ändern, markieren Sie das Modul in der Liste, klicken Sie auf **Ändern** und legen Sie im folgenden Fenster die gewünschte Aktion fest.

Beachten Sie, dass ein Trainingsvorgang ausgeführt wird, wenn eine zu kontrollierende Anwendung nach der Installation von Kaspersky Internet Security zum ersten Mal gestartet wird. Das Training dauert an, bis die Arbeit der Anwendung beendet wird. Während des Trainings wird eine Liste der von der Anwendung verwendeten Module erstellt. Die Regeln zur Integritätskontrolle werden bei den nachfolgenden Starts der Anwendung verwendet.

10.1.2.2. Erstellen einer Liste der gemeinsamen Komponenten

Kaspersky Internet Security verfügt über eine Liste von gemeinsamen Komponenten, die in alle zu kontrollierenden Anwendungen geladen werden dürfen. Diese Liste befindet sich auf der Registerkarte **Gemeinsame Komponenten** (s. Abb. 36). Die Liste enthält Module, die von Kaspersky Internet Security verwendet werden, Komponenten, die über eine Microsoft Corporation-Signatur verfügen, sowie vom Benutzer hinzugefügte Komponenten.

Damit die Module von Programmen, die Sie auf Ihrem Computer installieren und die über eine Microsoft Corporation-Signatur verfügen, automatisch zur Liste der vertrauenswürdigen Module hinzugefügt werden, aktivieren Sie das Kontrollkästchen ☑ **Komponenten mit Microsoft Corporation Signatur automatisch zur Liste hinzufügen**. Wenn in diesem Fall eine der Kontrolle unterliegende Anwendung versucht, ein Modul zu laden, das eine Microsoft Corporation-Signatur besitzt, wird das Laden dieses Moduls automatisch erlaubt und das Modul wird zur Liste der gemeinsamen Komponenten hinzugefügt.



Abbildung 36. Anpassen der Liste mit vertrauenswürdigen Modulen

Um der Liste ein vertrauenswürdiges Modul hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im Standardfenster zur Dateiauswahl das Modul.

10.1.3. Kontrolle der VBA-Makroausführung

Diese Komponente des Proaktiven Schutzes funktioniert nicht auf Computern mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64.

Die Untersuchung und Bearbeitung gefährlicher Makros, die auf Ihrem Computer gestartet werden sollen, wird durch das Kontrollkästchen ☑ **VBA-Makrountersuchung aktivieren** reguliert. Das Kontrollkästchen ist standardmäßig aktiviert. Die Aktivität jedes zu startenden Makros wird auf gefährliches Verhalten hin überwacht. Wenn eine gefährliche Aktivität erkannt wird, erlaubt oder sperrt der Proaktive Schutz die Makroausführung.

Beispiel:

Die Integration einer Leiste für Adobe Acrobat in die Anwendung Microsoft Office Word wird durch das Makro PDFMaker ausgeführt. Diese Leiste erlaubt es, aus einem beliebigen Dokument eine PDF-Datei zu erstellen. Eine Aktion wie die Integration von Elementen in ein Programm wird vom Proaktiven Schutz als gefährlich klassifiziert. Wenn die Kontrolle von VBA-Makros durch Kaspersky Internet Security aktiviert ist, erscheint beim Start des Makros auf dem Bildschirm eine Meldung des Proaktiven Schutzes, die Sie darüber informiert, dass ein gefährlicher Makrobefehl gefunden wurde. Sie können die Arbeit des Makros beenden und dadurch seine Ausführung abbrechen, oder sie erlauben.

Sie können festlegen, wie Kaspersky Internet Security auf das Ausführen verdächtiger Aktionen durch ein Makro reagieren soll. Wenn Sie überzeugt sind, dass das Ausführen verdächtiger Aktionen durch ein Makro bei der Arbeit mit einem konkreten Objekt (beispielsweise mit einem Microsoft Word-Dokument) kein gefährliches Ereignis darstellt, wird empfohlen, eine Ausnahmeregel zu erstellen. Wenn eine Situation eintritt, die den Bedingungen der Ausnahmeregel entspricht, wird die verdächtige Aktion, die vom Makro ausgeführt werden soll, vom Proaktiven Schutz nicht bearbeitet.

Um ins Konfigurationsfenster für die Makrountersuchung zu wechseln,

1. Öffnen Sie mit dem Link Einstellungen des Programmhauptfensters das Konfigurationsfenster von Kaspersky Internet Security.
2. Wählen Sie in der Konfigurationsstruktur die Komponente **Proaktiver Schutz**.
3. Klicken Sie im Block **Untersuchung von VBA-Makros** auf die Schaltfläche **Einstellungen**.

Die Bearbeitungsregeln für gefährliche Makros werden im Fenster **Einstellungen für VBA-Makrountersuchung** konfiguriert (s. Abb. 37). Es enthält standardmäßig Regeln für jene Aktionen, die von Kaspersky-Lab-Spezialisten als gefährlich klassifiziert werden. Zu diesen Aktionen zählen beispielsweise das Einfügen von Modulen in Programme und das Löschen von Dateien.

Wenn Sie eine in der Liste vorhandene verdächtige Aktionen für ungefährlich halten, deaktivieren Sie das Kontrollkästchen neben ihrem Namen. Dies kann beispielsweise der Fall sein, wenn Sie ständig mit einem Programm arbeiten, das ein Makro ausführt, das bestimmte Dateien zum Schreiben öffnet, und Sie völlig sicher sind, dass diese Operation keine Gefahr darstellt.

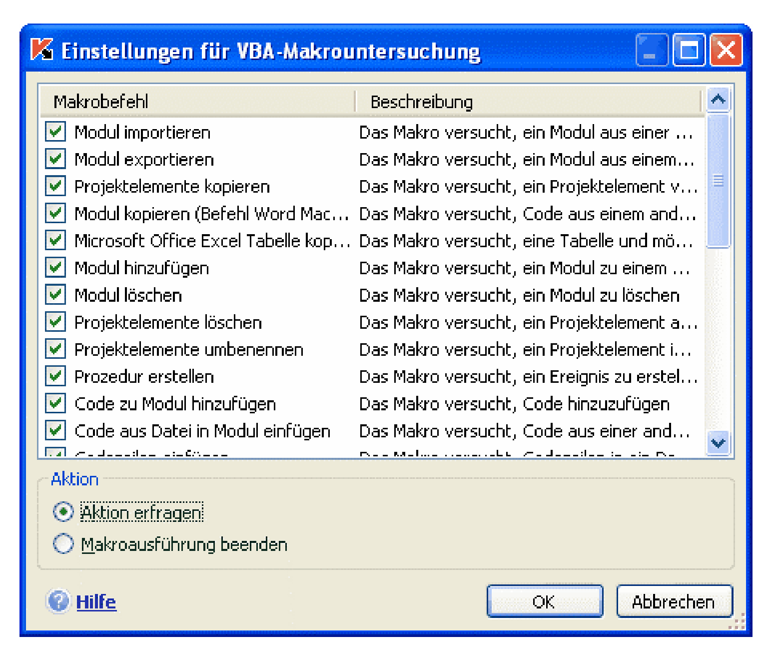


Abbildung 37. Einstellungen für die Untersuchung von VBA-Makros

Damit Kaspersky Internet Security die Ausführung eines Makros nicht blockiert,

> deaktivieren Sie das Kontrollkästchen neben der entsprechenden Aktion. Diese Aktion gilt dann als sicher und wird vom Proaktiven Schutz nicht bearbeitet.

Wenn eine von einem Makro initiierte verdächtige Aktion erkannt wird, zeigt die Anwendung standardmäßig eine Meldung auf dem Bildschirm an, in der angefragt wird, ob die Ausführung des Makros erlaubt oder verboten werden soll.

Damit die Anwendung die Ausführung aller gefährlichen Aktionen ohne vorherige Bestätigungsabfrage automatisch blockiert,

> wählen Sie in der Makro-Liste die Aktion **Makroausführung beenden**.

10.1.4. Kontrolle über Veränderungen der Systemregistrierung

Ein Ziel vieler schädlicher Programme besteht in einer Veränderung der Registrierung des Betriebssystems auf Ihrem Computer. Dabei kann es sich um

harmlose Scherzprogramme oder aber um gefährliche Schadprogramme handeln, die eine ernste Bedrohung für Ihren Computer darstellen.

Schädliche Programme können beispielsweise ihren Start in einen Registrierungsschlüssel eintragen, der dem automatischen Start von Anwendungen dient. Dadurch wird das schädliche Programm gleich nach dem Start des Betriebssystems automatisch gestartet.

Ein spezielles Modul des Proaktiven Schutzes überwacht die Veränderungen von Systemregistrierungsobjekten. Die Arbeit dieses Moduls wird durch das Kontrollkästchen ☑ **Überwachung der Systemregistrierung aktivieren** reguliert.

Um zur Konfiguration der Systemregistrierungskontrolle zu wechseln,

1. Öffnen Sie mit der Schaltfläche Einstellungen des Programmhauptfensters das Konfigurationsfenster von Kaspersky Internet Security.

2. Wählen Sie in der Konfigurationsstruktur die Komponente **Proaktiver Schutz**.

3. Klicken Sie im Block **Überwachung der Systemregistrierung** auf die Schaltfläche **Einstellungen**.

Eine Liste der Regeln für die Arbeit mit Registrierungsobjekten wurde bereits von den Kaspersky-Lab-Spezialisten erstellt und gehört zum Lieferumfang des Programms. Die Operationen mit den Registrierungsobjekten sind in logische Gruppen wie *System Security, Internet Security usw.* unterteilt. Jede Gruppe enthält Objekte der Systemregistrierung und Regeln für die Arbeit mit diesen. Die Liste wird zusammen mit dem Programmupdate aktualisiert.

Eine vollständige Liste der Regeln befindet sich im Fenster **Gruppen der Registrierungsschlüssel** (s. Abb. 38).

Jede Regelgruppe besitzt eine bestimmte Ausführungspriorität, die Sie mit Hilfe der Schaltflächen **Aufwärts** und **Abwärts** erhöhen oder vermindern können. Je höher die Position einer Gruppe in der Liste, desto höher ist ihre Ausführungspriorität. Wenn ein Registrierungsobjekt zu mehreren Gruppen gehört, wird zuerst die Regel aus der Gruppe mit der höchsten Priorität auf das Objekt angewandt.

Die Verwendung einer bestimmten Regelgruppe kann folgendermaßen aufgehoben werden:

- Deaktivieren des Kontrollkästchens ☑ neben dem Namen der Gruppe. In diesem Fall verbleibt die Regelgruppe in der Liste, wird aber nicht verwendet.

- Löschen der Regelgruppe aus der Liste. Es wird davor gewarnt, die von den Kaspersky-Lab-Spezialisten erstellten Gruppen zu löschen, weil sie

eine Liste der Systemregistrierungsobjekte enthalten, die am häufigsten von Schadprogrammen benutzt werden.



Abbildung 38. Zu kontrollierende Schlüssel der Systemregistrierung

Es besteht die Möglichkeit, eigene Gruppen für zu kontrollierende Systemregistrierungsobjekte zu erstellen. Klicken Sie dazu im Fenster der Objektgruppen auf die Schaltfläche **Hinzufügen**.

Nehmen Sie im nächsten Fenster folgende Einstellungen vor:

1. Geben Sie den Namen der neuen Gruppe von Systemregistrierungsobjekten im Feld **Gruppenname** an.

2. Erstellen Sie eine Liste mit den Objekten der Systemregistrierung, die der zu kontrollierenden Gruppe angehören sollen. Dazu dient die Registerkarte **Schlüssel** (s. Pkt. 10.1.4.1 auf S. 151). Dabei können ein oder mehrere Objekte verwendet werden.

3. Erstellen Sie eine Regel für die Objekte der Registrierung. Dazu dient die Registerkarte **Regeln** (s. Pkt. 10.1.4.2 auf S. 153). Sie können mehrere Regeln erstellen und ihre Anwendungspriorität bestimmen.

10.1.4.1. Auswahl von Registrierungsobjekten zum Erstellen einer Regel

Die erstellte Gruppe von Objekten muss mindestens ein Systemregistrierungsobjekt enthalten. Die Liste der Objekte für die Regel wird auf der Registerkarte **Schlüssel** angelegt.

Um ein Systemregistrierungsobjekt hinzuzufügen,

1. Klicken Sie im Fenster **Gruppe ändern** auf die Schaltfläche **Hinzufügen** (s. Abb. 39).
2. Wählen Sie im folgenden Fenster das Objekt oder die Gruppe von Objekten der Systemregistrierung, für die Sie eine Kontrollregel erstellen möchten.
3. Geben Sie im Feld **Wert** den Wert des Objekts oder die Maske der Gruppe von Objekten an, für welche(s) die Regel gelten soll.
4. Aktivieren Sie das Kontrollkästchen ☑ **Untergeordnete Schlüssel einschließen**, damit die Regel auf alle untergeordneten Schlüssel des gewählten Systemregistrierungsobjekts angewandt wird.

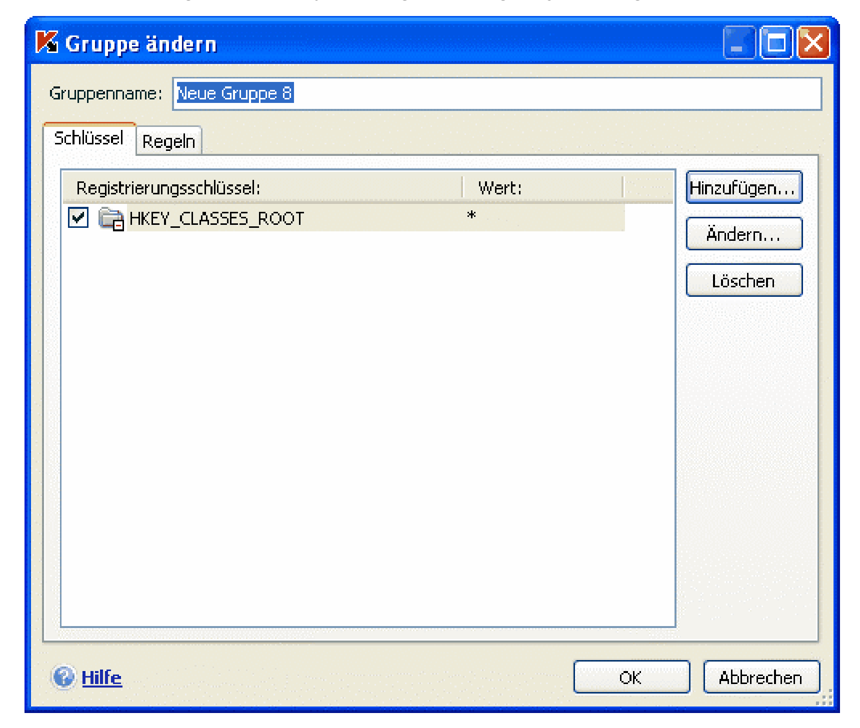


Abbildung 39. Hinzufügen eines Registrierungsschlüssels, der kontrolliert werden soll

Eine Maske mit den Zeichen * oder ? muss nur dann gleichzeitig mit dem Kontrollkästchen ☑ **Untergeordnete Schlüssel einschließen** verwendet werden, wenn diese Zeichen im Namen des Schlüssels vorhanden sind.

Wenn eine Gruppe von Registrierungsobjekten mit Hilfe einer Maske ausgewählt und dafür ein konkreter Wert angegeben wurde, wird die Regel streng auf den angegebenen Wert für jeden beliebigen Schlüssel der gewählten Gruppe angewandt.

10.1.4.2. Erstellen einer Regel zur Kontrolle von Registrierungsobjekten

Eine Kontrollregel für Systemregistrierungsobjekte besteht aus folgenden Parametern:

- Anwendung, für welche die Regel benutzt wird, wenn sie versucht, auf Systemregistrierungsobjekte zuzugreifen.
- Reaktion des Programms auf den Versuch der Anwendung, eine bestimmte Operation mit Systemregistrierungsobjekten auszuführen.

Um eine Regel für die ausgewählten Systemregistrierungsobjekte zu erstellen,

1. Klicken Sie auf der Registerkarte **Regeln** auf die Schaltfläche **Erstellen**. Die vordefinierte Regel wird an erster Stelle zur Regelliste hinzugefügt (s. Abb. 40).

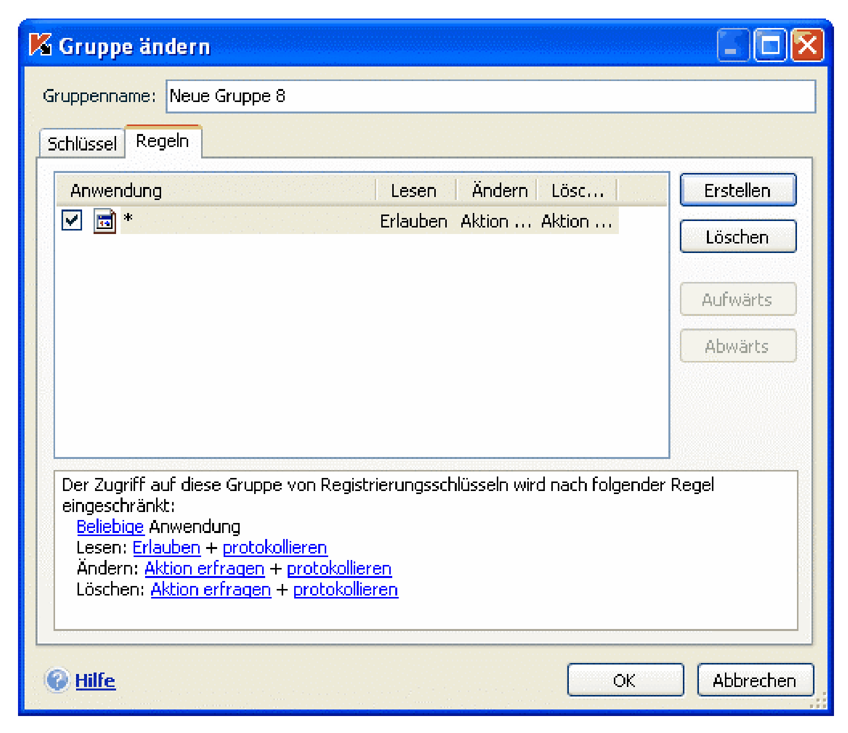


Abbildung 40. Erstellen einer Kontrollregel für Systemregistrierungsschlüssel

2. Markieren Sie die Regel in der Liste und legen Sie im unteren Bereich der Registerkarte die Parameter der Regel fest:

   - Geben Sie eine Anwendung an.

     Die Regel wird standardmäßig für eine beliebige Anwendung erstellt. Damit sich die Regel auf eine konkrete Anwendung bezieht, klicken Sie mit der linken Maustaste auf den Link Beliebige, der dadurch den Wert Ausgewählte annimmt. Verwenden Sie dann den Link Anwendung angeben. Dadurch öffnet sich ein Kontextmenü, in dem Sie mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl oder mit dem Punkt **Anwendungen** zur Liste der momentan aktiven Anwendungen wechseln können, um die gewünschte Anwendung auszuwählen.

   - Bestimmen Sie die Reaktion des Proaktiven Schutzes auf den Versuch der gewählten Anwendung, eine Operation zum Lesen, Ändern oder Löschen von Systemregistrierungsobjekten auszuführen.

Als Reaktion kann eine der folgenden Aktionen verwendet werden: erlauben, Aktion erfragen und verbieten. Klicken Sie mit der linken Maustaste auf den Link mit der Aktion, bis er den gewünschten Wert annimmt.

- Legen Sie fest, ob ein Bericht über die ausgeführte Operation erstellt werden soll. Verwenden Sie dazu den Link protokollieren/nicht protokollieren.

Sie können mehrere Regeln erstellen und deren Ausführungspriorität mit Hilfe der Schaltflächen **Aufwärts** und **Abwärts** festlegen. Je höher die Position einer Regel in der Liste, desto höher ist ihre Priorität.

Eine Erlaubnisregel für ein Systemregistrierungsobjekt kann auch aus der Meldung erstellt werden, die bei einer versuchten Operation mit dem Objekt erscheint. Verwenden Sie dazu in der Meldung den Link Erlaubnisregel erstellen und geben Sie im folgenden Fenster das Systemregistrierungsobjekt an, auf das sich die Regel beziehen soll.

KAPITEL 11. SCHUTZ VOR WERBUNG UND INTERNETBETRUG

Im Bereich der gefährlichen Software breiten sich in letzter Zeit immer mehr Programme aus, die folgende Ziele verfolgen:

- Diebstahl Ihrer vertraulichen Informationen (Kennwörter, Kreditkarten-nummern, wichtige Dokumente usw.).
- Überwachen Ihrer Aktionen auf dem Computer, Analyse der installierten Software.
- Aufdringliche Werbung mit unterschiedlichem Inhalt in Browserfenstern, Popup-Fenstern und auf Bannern bestimmter Programme.
- Unautorisierter Internetzugriff von Ihrem Computer aus auf Webseiten mit unterschiedlichem Inhalt.

Phishing-Angriffe und Tastaturspione verfolgen den Diebstahl von Informationen, Programme zur automatischen Einwahl zielen auf kostenpflichtige Webseiten, Scherzprogramme und Adware verschwenden Ihr Geld und Ihre Zeit. Die Aufgabe von *Anti-Spy* besteht im Schutz vor solchen Programmen.

Anti-Spy umfasst folgende Module:

- *Anti-Phishing* gewährleistet den Schutz vor Phishing-Angriffen.

  Phishing-Angriffe besitzen in der Regel die Form von E-Mail-Nachrichten, die scheinbar von Banken stammen und Links auf deren Webseiten enthalten. Der Nachrichtentext fordert dazu auf, einem Link zu folgen und auf der entsprechenden Webseite vertrauliche Informationen wie beispielsweise eine Kreditkartennummer oder den Namen und das Kennwort der persönlichen Online-Banking-Seite anzugeben, auf der finanzielle Operationen erfolgen können.

  Ein häufiges Beispiel für Phishing-Angriffe ist der Brief einer Bank, bei der Sie Kunde sind, mit einem Link auf deren offizielle Internetseite. Wenn der Link verwendet wird, gelangen Sie auf eine Webseite, die eine genaue Kopie der Bankseite darstellt und im Browser sogar deren Adresse anzeigen kann, obwohl Sie sich in Wirklichkeit auf einer fiktiven Seite befinden. Alle Aktionen, die Sie auf dieser Seite ausführen, werden verfolgt und können zum Diebstahl Ihres Geldes missbraucht werden.

Nicht nur E-Mails, sondern auch andere Mittel wie beispielsweise der Text einer ICQ-Nachricht können Links auf Phishing-Seiten enthalten. Anti-Phishing überwacht Versuche zum Öffnen von Phishing-Seiten und blockiert sie.

Die Bedrohungssignaturen von Kaspersky Internet Security enthalten die gegenwärtig bekannten Seiten, die für Phishing-Angriffe benutzt werden. Die Kaspersky-Lab-Spezialisten fügen ihnen Adressen hinzu, die von der internationalen Organisation zum Kampf gegen Phishing (The Anti-Phishing Working Group) zur Verfügung gestellt werden. Diese Liste wird beim Update der Bedrohungssignaturen ergänzt.

- *Popup-Blocker* blockiert den Zugriff auf Internetressourcen mit Werbeinformationen, beispielsweise das Öffnen von Popup-Fenstern.

  Die Informationen in den Popup-Fenstern sind in der Regel nicht nützlich. Solche Fenster werden automatisch geöffnet, wenn bestimmte Internetseiten besucht oder bestimmte Hyperlinks, die in ein anderes Fenster führen, verwendet werden. Sie enthalten Werbung und andere Informationen, deren Anzeige nicht von Ihnen initiiert wurde. Popup-Blocker blockiert das Öffnen solcher Fenster, worüber ein spezieller Hinweis über dem Programmsymbol im Infobereich der Taskleiste informiert. Direkt in diesem Hinweis können Sie bestimmen, ob Sie das Fenster blockieren möchten oder nicht.

  > Popup-Blocker arbeitet korrekt mit dem Modul zusammen, das in Microsoft Internet Explorer Popup-Fenster blockiert und zu Service Pack 2 für Microsoft Windows XP gehört. Bei der Programminstallation wird ein Erweiterungsmodul in den Browser integriert, das es erlaubt, das Öffnen von Popup-Fenstern direkt im Browser zu erlauben.

  Auf bestimmten Seiten werden Popup-Fenster allerdings verwendet, um den bequemen und schnellen Zugriff auf Informationen zu organisieren. Wenn Sie häufig mit solchen Seiten arbeiten und die Informationen der Popup-Fenster für Sie wichtig sind, wird empfohlen, sie zur Liste der vertrauenswürdigen Seiten hinzuzufügen (s. Pkt. 11.1.1 auf S. 159). Popup-Fenster auf vertrauenswürdigen Seiten werden nicht blockiert.

  Bei der Arbeit mit Microsoft Internet Explorer erscheint beim Blockieren eines Popup-Fensters in der Statusleiste des Browsers das Symbol . Durch Klick auf das Symbol können Sie entweder das Blockieren ablehnen oder die Adresse zur Liste der vertrauenswürdigen Adressen hinzufügen.

- *Anti-Banner* blockiert Werbung, die im Internet auf speziellen Bannern platziert oder in das Interface von auf Ihrem Computer installierten Programmen integriert ist.

Die Werbeinformationen auf den Bannern enthalten nicht nur unnütze Informationen, sondern lenken Sie auch von Ihrer Beschäftigung ab und erhöhen das Volumen der heruntergeladenen Datenmenge. Anti-Banner blockiert die momentan meistverbreiteten Banner, deren Masken im Lieferumfang von Kaspersky Internet Security enthalten sind. Sie können das Blockieren von Bannern abschalten oder eigene Listen mit erlaubten und verbotenen Bannern erstellen.

> Um das Modul Anti-Banner in den Browser **Opera** zu integrieren, fügen Sie der Datei *standard_menu.ini* im Abschnitt **[Image Link Popup Menu]** folgende Zeile hinzu:
>
> ```
> Item, "New banner" = Copy image address & Execute program, "<Laufwerk>\Program Files\Kaspersky Lab\Kaspersky Internet Security 6.0\opera_banner_deny.vbs", "//nologo %C"
> ```

- *Anti-Dialer* bietet Schutz vor Versuchen zu einer unerlaubten Modemverbindung.

> Anti-Dialer funktioniert auf den Betriebssystemen Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows XP x64, Microsoft Windows Vista und Microsoft Windows Vista x64.

In der Regel stellen Dialer eine Verbindung mit bestimmten Webseiten her, die beispielsweise pornografischen Charakter besitzen. Als Folge sind Sie gezwungen, hohe Rechnungen für den Datenaustausch zu bezahlen, der überhaupt nicht von Ihnen initiiert wurde. Wenn Sie eine bestimmte Nummer aus der Sperrliste ausschließen möchten, nehmen Sie die Nummer in die Liste der vertrauenswürdigen Nummern auf (s. Pkt. 11.1.3 auf S. 164).

11.1. Konfiguration von Anti-Spy

Der Schutz vor Internetbetrug und aufdringlicher Werbung berücksichtigt alle den Kaspersky-Lab-Spezialisten bekannten Programme, die zum Diebstahl von vertraulichen Informationen benutzt werden, und damit zu finanziellen Verlusten führen können. Die Komponente kann in folgender Hinsicht genau konfiguriert werden:

- Erstellen einer Liste vertrauenswürdiger Webseitenadressen (s. Pkt. 11.1.1 auf S. 159), deren Popup-Fenster nicht blockiert werden sollen.
- Erstellen einer weißen und schwarzen Bannerliste (s. Pkt. 11.1.2 auf S. 161).

- Erstellen einer Liste mit auszuschließenden Telefonnummern (s. Pkt. 11.1.3 auf S. 164), mit denen Sie Dial-up-Verbindungen erlauben.

11.1.1. Erstellen einer Liste mit vertrauenswürdigen Adressen für Popup-Blocker

Popup-Blocker blockiert standardmäßig ohne Bestätigungsabfrage die meisten Popup-Fenster, die automatisch geöffnet werden. Eine Ausnahme stellen die Popup-Fenster von Webseiten dar, die zur Liste der vertrauenswürdigen Seiten in Microsoft Internet Explorer und der Seiten des lokalen Netzwerks (Intranet), in dem Sie gerade angemeldet sind, gehören.

Wenn auf Ihrem Computer das Betriebssystem Microsoft Windows XP mit Service Pack 2 installiert ist, enthält Microsoft Internet Explorer einen eigenen Blocker für Popup-Fenster. Sie können dessen Arbeit konfigurieren, indem Sie auswählen, welche Fenster Sie blockieren möchten und welche nicht. Popup-Blocker unterstützt die Zusammenarbeit mit diesem Blocker nach folgendem Prinzip: Beim Versuch, ein Popup-Fenster zu öffnen, besitzt eine Verbotsregel stets den Vorrang. Ist beispielsweise die Adresse eines bestimmten Popup-Fensters in der Liste der zugelassenen Fenster für Microsoft Internet Explorer vorhanden, zählt aber nicht zu den vertrauenswürdigen Adressen von Popup-Blocker, dann wird das Fenster blockiert. Wenn im umgekehrten Fall im Browser festgelegt wurde, dass alle Popup-Fenster blockiert werden, dann wird die Adresse eines Fensters selbst dann blockiert, wenn sie zur Liste der vertrauenswürdigen Adressen von Popup-Blocker gehört. Deshalb ist es bei der Arbeit mit Microsoft Windows XP Service Pack 2 empfehlenswert, den Browser und Popup-Blocker aufeinander abzustimmen.

Wenn Sie möchten, dass bestimmte Popup-Fenster angezeigt werden, fügen Sie diese auf folgende Weise zur Liste der vertrauenswürdigen Adressen hinzu:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security und wählen Sie in der Konfigurationsstruktur **Anti-Spy**.

2. Klicken Sie im Abschnitt für das Blockieren von Popup-Fenstern auf die Schaltfläche **Vertrauenswürdige Adressen**.

3. Klicken Sie im folgenden Fenster (s. Abb. 41) auf die Schaltfläche **Hinzufügen** und geben Sie eine Maske für die Seiten an, deren Popup-Fenster nicht blockiert werden sollen.

> Hinweis.
>
> Zur Angabe der Maske einer vertrauenswürdigen Adresse sind die Zeichen ***** und **?** zulässig.

Beispiel: Die Maske http://www.test* schließt die Popup-Fenster aller Seiten aus, die mit der angegebenen Zeichenfolge beginnen.

4. Legen Sie fest, ob Adressen, die der vertrauenswürdigen Zone von Microsoft Internet Explorer angehören oder Adressen Ihres lokalen Netzwerks sind, von der Untersuchung ausgeschlossen werden sollen. Das Programm betrachtet sie standardmäßig als vertrauenswürdig und blockiert die Popup-Fenster dieser Adressen nicht.

Die neue Ausnahme wird an erster Stelle zur Liste der vertrauenswürdigen Adressen hinzugefügt. Damit eine von Ihnen hinzugefügte Ausnahme nicht verwendet wird, ist es ausreichend, das Kontrollkästchen ☑ neben ihrem Namen zu deaktivieren. Wenn Sie eine bestimmte Ausnahme verwerfen möchten, markieren Sie diese in der Liste und verwenden Sie die Schaltfläche **Löschen**.

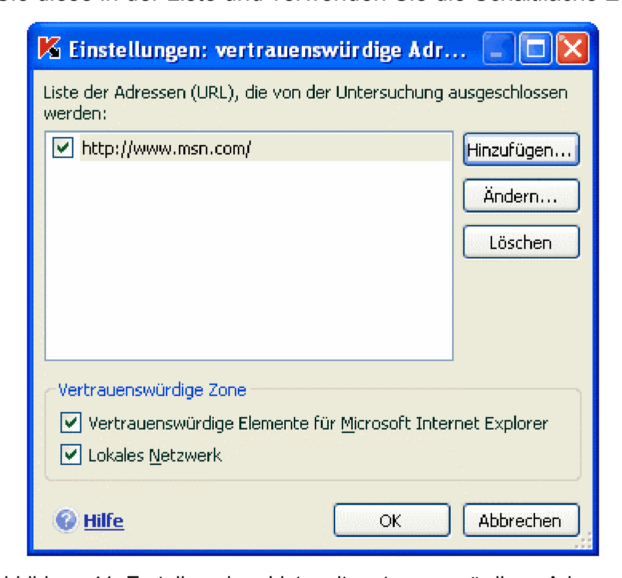


Abbildung 41. Erstellen einer Liste mit vertrauenswürdigen Adressen

Wenn Sie Popup-Fenster des Intranets und der Webseiten, die zur Liste der vertrauenswürdigen Seiten für Microsoft Internet Explorer gehören, blockieren möchten, deaktivieren Sie die entsprechenden Kontrollkästchen im Abschnitt **Vertrauenswürdige Zone**.

Beim Öffnen von Popup-Fenstern, die nicht zur vertrauenswürdigen Liste gehören, wird über dem Programmsymbol eine Meldung eingeblendet, die über das Blockieren des Fensters benachrichtigt. Mit Hilfe der Links in dieser Meldung können Sie das Blockieren ablehnen und die Adresse des Fensters in die Liste der vertrauenswürdigen aufnehmen.

Die entsprechenden Aktionen können Sie auch bei der Arbeit in Microsoft Internet Explorer ausführen, der zu Microsoft Windows XP mit Service Pack 2 gehört. Verwenden Sie dazu das Kontextmenü, das durch Klick auf das Programmsymbol geöffnet wird. Das Programmsymbol erscheint beim Blockieren von Popup-Fenstern im unteren Bereich des Browserfensters.

11.1.2. Adressenliste für zu blockierende Banner

Eine Liste mit Masken der häufigsten Werbebanner wurde von den Kaspersky-Lab-Spezialisten auf der Basis spezieller Untersuchungen erstellt und in den Lieferumfang des Programms aufgenommen. Die Werbebanner, die einer Maske dieser Liste entsprechen, werden vom Programm blockiert, falls das Blockieren von Bannern nicht deaktiviert wurde.

Außerdem können Sie eine weiße und schwarze Bannerliste anlegen, auf deren Grundlage der Empfang von Bannern erlaubt bzw. verboten wird.

Beachten Sie, dass der Zugriff auf den Stamm einer Seite nicht blockiert wird, wenn eine Maske der Domäne in der Liste der verbotenen Banner oder in der schwarzen Liste steht.

Wenn die Liste der verbotenen Banner beispielsweise die Maske **truehits.net** enthält, wird der Zugriff auf die Seite **http://truehits.net** erlaubt, während der Zugriff auf **http://truehits.net/a.jpg** blockiert wird.

11.1.2.1. Konfiguration der Standardliste für zu blockierende Banner

Kaspersky Internet Security umfasst eine Liste der Masken der meistverbreiteten Banner, die auf Webseiten im Internet und auf Benutzeroberflächen bestimmter Programme gestartet werden. Diese Liste wurde von den Kaspersky-Lab-Spezialisten erstellt und wird zusammen mit den Bedrohungssignaturen aktualisiert.

Sie können wählen, welche standardmäßigen Bannermasken Sie bei der Arbeit von Anti-Banner verwenden möchten. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security und wählen Sie in der Konfigurationsstruktur **Anti-Spy**.
2. Klicken Sie im Abschnitt für das Blockieren von Werbebannern auf die Schaltfläche **Einstellungen**.

3. Öffnen Sie die Registerkarte **Allgemein** (s. Abb. 42). Die auf der Registerkarte angegebenen Bannermasken werden von Anti-Banner blockiert. Die Maskenzeile kann an einer beliebigen Stelle der Banneradresse stehen.

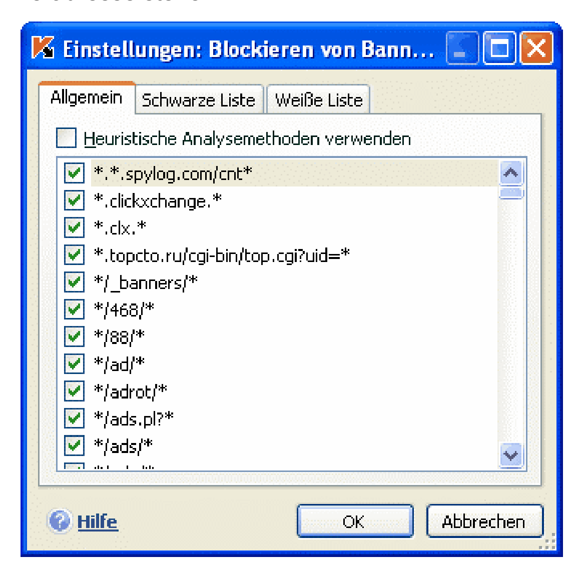


Abbildung 42. Liste mit zu blockierenden Bannern

Die Liste der standardmäßig zu blockierenden Masken steht nicht für Änderungen zur Verfügung. Wenn Sie ein Banner, das einer bestimmten Standardmaske entspricht, nicht blockieren möchten, entfernen Sie das Kontrollkästchen neben der Maske.

Zur Analyse von Bannern, die nicht unter die Masken der Standardliste fallen, aktivieren Sie das Kontrollkästchen **Heuristische Analysemethoden verwenden**. In diesem Fall werden heruntergeladene Bilder von der Anwendung auf das Vorhandensein von charakteristischen Bannermerkmalen analysiert. Aufgrund dieser Analyse können Bilder als Banner identifiziert und blockiert werden.

Außerdem können Sie eigene Listen für erlaubte und verbotene Banner anlegen. Dazu dienen die Registerkarten **Weiße Liste** und **Schwarze Liste**.

11.1.2.2. Weiße Bannerliste

Die weiße Bannerliste wird vom Benutzer während der Arbeit mit dem Programm erstellt, wenn bestimmte Banner nicht blockiert werden sollen. Diese Liste enthält die für den Empfang zugelassenen Banner.

Um eine neue Maske zur weißen Liste hinzuzufügen:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security und wählen Sie in der Konfigurationsstruktur **Anti-Spy**.
2. Klicken Sie im Abschnitt für das Blockieren von Werbebannern auf die Schaltfläche **Einstellungen**.
3. Öffnen Sie die Registerkarte **Weiße Liste**.

Tragen Sie mit der Schaltfläche **Hinzufügen** die Maske des erlaubten Banners ein. Sie können die vollständige Adresse (URL) des Banners oder seine Maske angeben. Im letzten Fall wird beim Versuch zum Öffnen eines Banners seine Adresse nach der angegebenen Maske durchsucht.

Bei der Angabe einer Bannermaske können die Symbole ***** und **?** benutzt werden (wobei * für eine beliebige Zeichenfolge und ? für ein beliebiges Einzelzeichen steht).

Damit eine von Ihnen hinzugefügte Maske nicht verwendet wird, müssen Sie diese nicht unbedingt aus der Liste löschen. Es ist ausreichend, das entsprechende Kontrollkästchen ☑ zu deaktivieren.

Mit Hilfe der Schaltflächen **Import** und **Export** können Sie die erstellten schwarzen Bannerlisten von einem Computer auf einen anderen kopieren.

11.1.2.3. Schwarze Bannerliste

Zusätzlich zu der Liste der standardmäßigen Bannermasken (s. Pkt. 11.1.2.1 auf S. 161), die von Anti-Banner blockiert werden, können Sie eine eigene Liste anlegen. Gehen Sie folgendermaßen vor:

4. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security und wählen Sie in der Konfigurationsstruktur **Anti-Spy**.
5. Klicken Sie im Abschnitt für das Blockieren von Werbebannern auf die Schaltfläche **Einstellungen**.
6. Öffnen Sie die Registerkarte **Schwarze Liste**.

Tragen Sie mit der Schaltfläche **Hinzufügen** die Maske des Banners ein, das von Anti-Banner blockiert werden soll. Sie können die vollständige Adresse

(URL) des Banners oder eine Zeichenfolge angeben. Im letzten Fall wird beim Versuch zum Öffnen eines Banners seine Adresse nach der festgelegten Zeichenfolge untersucht.

> Bei der Angabe einer Bannermaske können die Symbole ***** und **?** benutzt werden (wobei * für eine beliebige Zeichenfolge und ? für ein beliebiges Einzelzeichen steht).

Damit eine von Ihnen hinzugefügte Maske nicht verwendet wird, müssen Sie diese nicht unbedingt aus der Liste löschen. Es ist ausreichend, das entsprechende Kontrollkästchen ☑ zu deaktivieren.

Mit Hilfe der Schaltflächen **Import** und **Export** können Sie die erstellten schwarzen Bannerlisten von einem Computer auf einen anderen kopieren.

11.1.3. Erstellen einer Liste mit vertrauenswürdigen Nummern für Anti-Dialer

Das Modul Anti-Dialer kontrolliert Telefonnummern, über die versteckte Internetverbindungen ausgeführt werden. Als versteckt gelten Verbindungen, in deren Einstellungen festgelegt ist, den Benutzer nicht über die Verbindung zu benachrichtigen, sowie Verbindungen, die nicht von Ihnen initiiert wurden.

Jedes Mal, wenn ein Versuch zu einer versteckten Verbindung erfolgt, erscheint auf dem Bildschirm ein spezieller Hinweis, der Sie darüber informiert. In diesem Hinweis werden Sie aufgefordert zu entscheiden, ob die Verbindung erlaubt oder verboten werden soll. Wenn Sie diese Verbindung nicht initiiert haben, ist es sehr wahrscheinlich, dass es sich um die Aktion eines schädlichen Programms handelt.

Wenn Sie Verbindungen über bestimmte Nummern ohne vorherige Anfrage des Programms zulassen möchten, fügen Sie diese folgendermaßen zur Liste der vertrauenswürdigen Nummern hinzu:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security und wählen Sie in der Konfigurationsstruktur **Anti-Spy**.

2. Klicken Sie im Abschnitt für das Blockieren von automatischen Einwahlversuchen auf die Schaltfläche **Vertrauenswürdige Nummern**.

3. Klicken Sie im folgenden Fenster (s. Abb. 43) auf die Schaltfläche **Hinzufügen** und geben Sie die Nummer oder eine Maske der Nummer an, für die eine Verbindung erlaubt werden soll.



Abbildung 43. Erstellen einer Liste mit vertrauenswürdigen Adressen

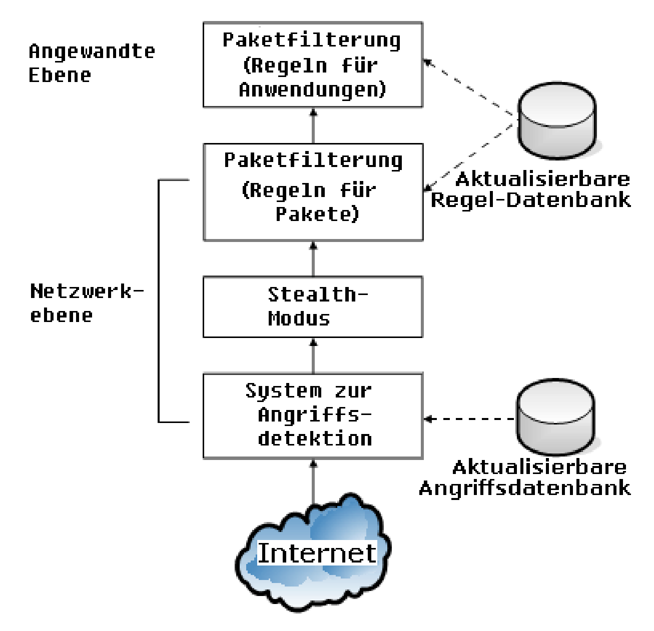
> Hinweis.
> Zur Angabe der Maske einer vertrauenswürdigen Nummer sind die Zeichen ***** und **?** zulässig.
> Beispiel: Die Maske *???79787** erstreckt sich auf alle Nummern, die mit den Ziffern *79787* beginnen, wobei die Vorwahl aus drei beliebigen Ziffern bestehen kann.

Die neue Ausnahme wird an erster Stelle zur Liste der vertrauenswürdigen Nummern hinzugefügt. Damit eine von Ihnen hinzugefügte Nummer nicht verwendet wird, ist es ausreichend, in der Liste das entsprechende Kontrollkästchen ☑ zu deaktivieren. Wenn Sie eine bestimmte Ausnahme verwerfen möchten, markieren Sie diese in der Liste und verwenden Sie die Schaltfläche **Löschen**.

KAPITEL 12. SCHUTZ VOR NETZWERKANGRIFFEN

Das Risiko, bei der Arbeit im Internet angegriffen zu werden, ist heutzutage relativ hoch. Ein Computer kann nicht nur von Viren infiziert werden, sondern wird auch durch unterschiedliche Arten von Angriffen gefährdet, die Schwachstellen in Betriebssystemen und Software ausnutzen.

Anti-Hacker ist eine spezielle Komponente von Kaspersky Internet Security, die der Sicherheit Ihrer Arbeit in lokalen Netzwerken und im Internet dient. Er schützt Ihren Computer auf Netzwerk- und Anwendungsebene, und gewährleistet zur Vorbeugung gegen Angriffe außerdem die Unsichtbarkeit des Computers in einem Netzwerk. Im Folgenden wird genauer beschrieben, worauf die Arbeit von Anti-Hacker basiert.



Der Schutz auf <u>Netzwerkebene</u> wird durch die Verwendung globaler Regeln für Netzwerkpakete gewährleistet. Dabei wird die Netzwerkaktivität auf Basis der Analyse von Parametern wie Paketrichtung, Übertragungsprotokoll des Pakets und Ziel- oder Ursprungsport eines Pakets erlaubt oder verboten. Die Paketregeln bestimmen die Möglichkeit des Netzwerkzugriffs unabhängig von den auf Ihrem Computer installierten Netzwerkanwendungen.

Zusätzlich zu den Paketregeln wird der Schutz auf Netzwerkebene durch ein *Subsystem zum Erkennen von Angriffen* (Intrusion Detection System – IDS) gewährleistet. Die Aufgabe dieses Subsystems besteht in der Analyse eingehender Verbindungen, im Erkennen von Versuchen zum Scannen der Ports Ihres Computers und in der Filterung von Netzwerkpaketen, die auf die Ausnutzung von Softwareschwachstellen gerichtet sind. Wenn das Subsystem einen Angriff erkennt, werden alle eingehenden Verbindungen mit dem angreifenden Computer für einen bestimmten Zeitraum blockiert und der Benutzer wird darüber informier, dass sein Computer aus dem Netzwerk angegriffen wurde.

Bei der Arbeit des Subsystems zur Angriffsdetektion wird zur Analyse eine spezielle Angriffsdatenbank (s. Pkt. 12.9 auf S. 187) verwendet, die von den Kaspersky-Lab-Spezialisten ständig ergänzt und gemeinsam mit den Bedrohungssignaturen aktualisiert wird.

Der Schutz auf der Anwendungsebene beruht auf Regeln für die Verwendung von Netzwerkressourcen durch die auf Ihrem Computer installierten Anwendungen. Wie der Schutz auf Netzwerkebene baut der Schutz auf der Anwendungsebene auf der Analyse von Netzwerkpaketen auf, wobei Paketrichtung, Typ des Übertragungsprotokolls und der verwendete Port berücksichtigt werden. Auf der Anwendungsebene werden allerdings nicht nur Merkmale eines Netzwerkpakets, sondern auch die konkrete Anwendung beachtet, an welche das Paket adressiert ist oder welche das Senden des Pakets initiierte.

Die Verwendung von Regeln für Anwendungen ermöglicht die genaue Konfiguration des Schutzes, wenn beispielsweise ein bestimmter Verbindungstyp für manche Anwendungen verboten, für andere aber erlaubt ist.

Ausgehend von den beiden Schutzebenen von Anti-Hacker existieren zwei Typen von Regeln:

- Regeln für Pakete (s. Pkt. 12.3 auf S. 175) werden verwendet, um unabhängig von den installierten Anwendungen generelle Beschränkungen der Netzwerkaktivität festzulegen. Beispiel: Wenn eine Paketregel erstellt wird, die eingehende Verbindungen auf Port 21 verbietet, besteht von außen kein Zugriff auf eine Verbindung, die diesen Port verwendet (beispielsweise ftp-Server).
- Regeln für Anwendungen (s. Pkt. 12.2 auf S. 170) werden verwendet, um die Netzwerkaktivität einer konkreten Anwendung einzuschränken. Beispiel: Wenn für alle Anwendungen eine Verbotsregel für Verbindungen auf Port 80 besteht, können sie eine Regel erstellen, welche die Verbindung unter Verwendung dieses Ports nur für den Webbrowser Firefox erlaubt.

Für Anwendungen und Pakete können *Erlaubnis*- und *Verbotsregeln* erstellt werden. Im Lieferumfang des Programms sind bestimmte Standardregeln

enthalten, welche die Netzwerkaktivität der verbreiteten Anwendungen und die Arbeit des Computers mit gebräuchlichen Protokollen und Ports regeln. Außerdem enthält Kaspersky Internet Security eine Auswahl von Erlaubnisregeln für vertrauenswürdige Anwendungen, deren Netzwerkaktivität ungefährlich ist.

Zur Vereinfachung der Konfiguration und Verwendung von Regeln in Kaspersky Internet Security wird die gesamte Netzwerkumgebung in *Sicherheitszonen* unterteilt, die häufig mit Subnetzen identisch sind, zu denen der Computer gehört. Sie können jeder Zone einen Status zuweisen (Internet, Lokales Netzwerk, Vertrauenswürdig), auf dessen Grundlage eine Richtlinie für die Verwendung von Regeln und die Kontrolle der Netzwerkaktivität in dieser Zone festgelegt wird (s. Pkt. 12.6 auf S. 181).

Ein spezieller Funktionsmodus von Anti-Hacker, der *Stealth-Modus*, verhindert, dass der Computer von außen erkannt werden kann. Dadurch verlieren Hacker ihr Angriffsobjekt. Gleichzeitig beeinträchtigt der Modus aber Ihre Arbeit im Internet in keiner Weise (unter der Voraussetzung, dass Ihr Computer nicht als Server dient).

12.1. Auswahl der Schutzstufe für Anti-Hacker

Der Schutz Ihrer Arbeit in einem Netzwerk erfolgt auf einer der folgenden Stufen (s. Abb. 44):

Alle blockieren – Diese Schutzstufe verbietet jede Netzwerkaktivität auf Ihrem Computer. Wenn diese Schutzstufe eingestellt ist, können Sie keine Netzwerkressourcen verwenden und Programme, für deren Arbeit eine Netzwerkverbindung erforderlich ist, funktionieren nicht. Diese Stufe wird nur für den Fall von Netzwerkangriffen oder bei der Arbeit des Computers in einer ungeschützten Umgebung empfohlen.

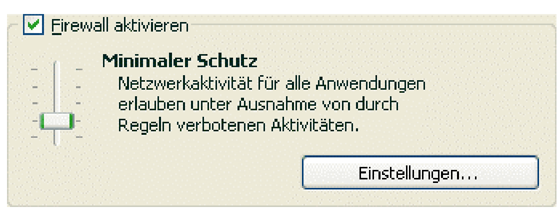


Abbildung 44. Auswahl der Sicherheitsstufe für den Netzwerkschutz

Maximaler Schutz – Diese Schutzstufe erlaubt die Netzwerkaktivität, für die eine Erlaubnisregel vorgesehen ist. Anti-Hacker verwendet die Regeln, die im Lieferumfang enthalten sind und von Ihnen erstellt wurden. Die Auswahl von Regeln, die zusammen mit Kaspersky Internet Security

geliefert wird, umfasst Erlaubnisregeln für die Anwendungen, deren Netzwerkaktivität nicht verdächtig ist, und für die Datenpakete, deren Empfang/Übertragung absolut sicher ist. Ist aber für die Anwendung in der Regelliste eine Verbotsregel mit höherer Priorität als die der Erlaubnisregel vorhanden, dann wird die Netzwerkaktivität dieser Anwendung verboten.

> Achtung!
>
> Auf dieser Schutzstufe wird jede Anwendung, deren Netzwerkaktivität nicht in einer Anti-Hacker-Erlaubnisregel definiert ist, blockiert. Deshalb wird die Verwendung dieser Stufe nur dann empfohlen, wenn Sie sicher sind, dass alle für Ihre Arbeit notwendigen Programme durch entsprechende Regeln erlaubt werden, und Sie nicht planen, neue Programme zu installieren.

Trainingsmodus – Schutzstufe, auf der die Anti-Hacker-Regeln erstellt werden. Auf dieser Stufe überprüft Anti-Hacker jedes Mal, wenn ein Programm versucht auf Netzwerkressourcen zuzugreifen, ob eine Regel für die Verbindung vorhanden ist. Wenn eine Regel existiert, verfährt Anti-Hacker nach deren Bedingungen. Ist keine Regel vorhanden, dann erscheint auf dem Bildschirm eine Meldung, die eine Beschreibung der Netzwerkverbindung enthält (initiierendes Programm, Port, Protokoll usw.). Sie werden aufgefordert zu entscheiden, ob diese Verbindung erlaubt oder verboten werden soll. Mit Hilfe einer speziellen Schaltfläche können Sie im Meldungsfenster eine Regel für die Verbindung erstellen, damit Anti-Hacker bei einer entsprechenden Verbindung die darin angegebenen Bedingungen benutzt, ohne eine Bildschirmmeldung anzuzeigen.

Minimaler Schutz – Auf dieser Schutzstufe wird nur die ausdrücklich verbotene Netzwerkaktivität blockiert. Anti-Hacker blockiert die Netzwerkaktivität in Übereinstimmung mit den Verbotsregeln, die im Lieferumfang enthalten sind und von Ihnen erstellt wurden. Ist für die Anwendung in der Regelliste allerdings eine Erlaubnisregel mit höherer Priorität als die Verbotsregel vorhanden, dann wird die Netzwerkaktivität dieser Anwendung zugelassen.

Alle erlauben – Diese Schutzstufe erlaubt jede beliebige Netzwerkaktivität auf Ihrem Computer. Es wird empfohlen, diese Stufe möglichst selten und nur dann zu wählen, wenn keine aktiven Netzwerkangriffe beobachtet werden und Sie jeder beliebigen Netzwerkaktivität absolut vertrauen.

Sie können die Schutzstufe Ihrer Arbeit in einem Netzwerk erhöhen oder verringern. Wählen Sie dazu die entsprechende Stufe oder ändern Sie die Parameter der aktuellen Stufe.

Um die Stufe des Netzwerkschutzes zu ändern,

1. Wählen Sie im Konfigurationsfenster von Kaspersky Internet Security die Komponente **Anti-Hacker**.
2. Verschieben Sie im Abschnitt Firewall den Zeiger auf der Skala.

Um eine Stufe des Netzwerkschutzes anzupassen,

1. Wählen Sie die Schutzstufe, die Ihren Anforderungen am nächsten kommt.
2. Klicken Sie auf die Schaltfläche **Einstellungen** und nehmen Sie im folgenden Fenster die Einstellungen für die Firewall vor.

12.2. Regeln für Anwendungen

Der Lieferumfang von Kaspersky Internet Security umfasst eine Sammlung von Regeln für die unter dem Betriebssystem Microsoft Windows verbreiteten Anwendungen. Für ein Programm können mehrere Erlaubnis- und Verbotsregeln vorhanden sein. In der Regel handelt es sich dabei um Programme, deren Netzwerkaktivität von den Kaspersky-Lab-Spezialisten ausführlich analysiert und als gefährlich oder ungefährlich eingestuft wurde.

Abhängig von der Schutzstufe (s. Pkt. 12.1 auf S. 168), die für die Arbeit der Firewall gewählt wurde, und dem Typ des Netzwerks (s. Pkt. 12.4 auf S. 177), in dem der Computer arbeitet, wird die Liste für die Programme auf unterschiedliche Weise verwendet. Auf der Stufe **Maximaler Schutz** wird jede von Anwendungen initiierte Netzwerkaktivität, die nicht unter die Erlaubnisregeln fällt, blockiert.

Um mit der Regelliste für Anwendungen zu arbeiten,

1. Klicken Sie im Abschnitt Firewall des Konfigurationsfensters von Anti-Hacker auf die Schaltfläche **Einstellungen**.
2. Wählen Sie im folgenden Fenster die Registerkarte **Regeln für Anwendungen** (s. Abb. 45).

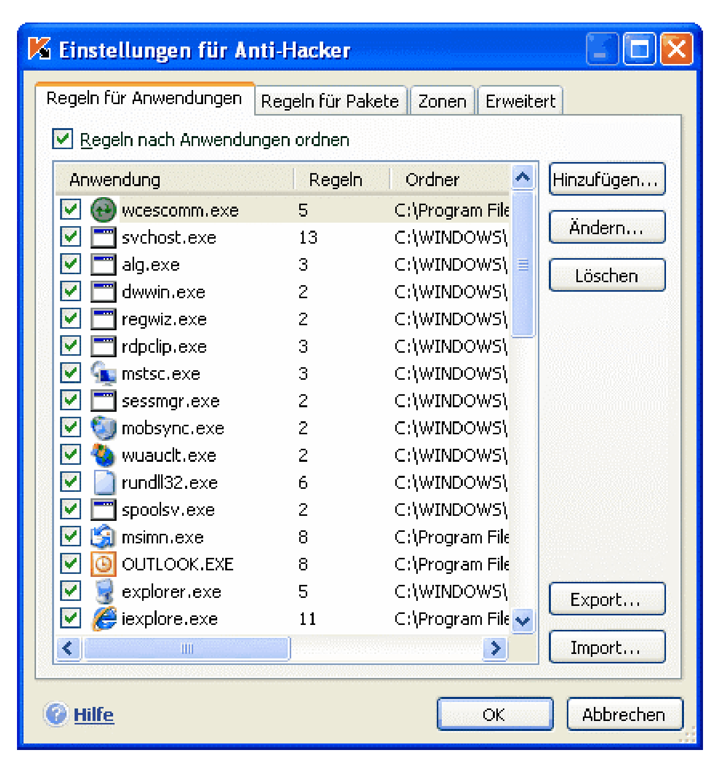


Abbildung 45. Liste der Regeln für die auf dem Computer installierten Anwendungen

Alle Regeln auf dieser Registerkarte lassen sich auf eine der folgenden Arten gruppieren:

- *Regeln für Anwendungen*. Wenn das Kontrollkästchen **Regeln nach Anwendungen ordnen** aktiviert ist, wird die Regelliste auf diese Weise angezeigt. Die Registerkarte enthält eine Liste der Anwendungen, für die Regeln vorhanden sind. Für jede Anwendung werden folgende Informationen angezeigt: Name und Symbol der Anwendung, Befehlszeile, Stammverzeichnis, in dem sich die ausführbare Datei der Anwendung befindet, und Anzahl der für die Anwendung erstellten Regeln.

  Mit der Schaltfläche **Ändern** gelangen Sie zu der Regelliste für die in der Liste gewählte Anwendung und können die Regelliste anpassen: neue Regeln hinzufügen, vorhandene Regeln und ihre Ausführungspriorität ändern.

  Mit der Schaltfläche **Hinzufügen** können Sie der Liste eine neue Anwendung hinzufügen und Regeln dafür erstellen.

Die Schaltflächen **Export** und **Import** dienen der Übertragung von erstellten Regeln auf andere Computer. Das ist nützlich zur schnellen Konfiguration von Anti-Hacker.

- *Allgemeine Regelliste* ohne Gruppierung nach Anwendungsnamen. Auf diese Weise wird die Regelliste dargestellt, wenn das Kontrollkästchen ☑ **Regeln nach Anwendungen ordnen** deaktiviert ist. Die allgemeine Liste gibt vollständige Informationen über die Regeln wieder: Neben dem Namen der Anwendung und der Befehlszeile für ihren Start werden die Aktion der Regel (Netzwerkaktivität erlauben oder verbieten), das Datenübertragungsprotokoll, die Richtung des Datenstroms (eingehend oder ausgehend) und andere Informationen angegeben.

  Mit der Schaltfläche **Hinzufügen** können Sie eine neue Regel erstellen. Mit der Schaltfläche **Ändern** können Sie zum Anpassen der aus der Liste gewählten Regeln wechseln. Die wichtigsten Parameter der Regel können auch im unteren Bereich der Registerkarte geändert werden.

  Mit Hilfe der Schaltflächen **Aufwärts** und **Abwärts** können Sie die Ausführungspriorität der Regel ändern.

12.2.1. Manuelles Erstellen einer Regel

Um eine Regel für eine Anwendung manuell zu erstellen,

1. Wählen Sie die Anwendung aus. Klicken Sie dazu auf der Registerkarte **Regeln für Anwendungen** auf die Schaltfläche **Hinzufügen**. Wählen Sie im folgenden Fenster die ausführbare Datei der Anwendung, für welche die Regel erstellt werden soll. Dadurch wird die Regelliste für die gewählte Anwendung geöffnet. Wenn bereits Regeln für sie vorhanden sind, werden diese im oberen Bereich des Fensters angezeigt. Wenn keine Regeln vorhanden sind, ist das Regelfenster leer.

   > Die Anwendung kann später gewählt werden, wenn die Regelbedingungen konfiguriert werden.

2. Klicken Sie im Regelfenster für die Anwendung auf die Schaltfläche **Hinzufügen**.

Im folgenden Fenster **Neue Regel** kann die neue Regel erstellt und detailliert angepasst werden (s. 12.4 Auf S. 177).

12.2.2. Erstellen einer Regel nach einer Vorlage

Zum Lieferumfang der Anwendung gehören fertige Regelvorlagen, die Sie zum Erstellen eigener Regeln verwenden können.

Die Vielzahl der existierenden Netzwerkanwendungen lässt sich bedingt in mehrere Typen wie Mailprogramme, Webbrowser usw. unterteilen. Für jeden Typ ist eine spezifische Aktivität charakteristisch (beispielsweise Empfang und Senden von E-Mails, Empfang und Anzeige von HTML-Seiten). Jeder Typ verwendet eine bestimmte Auswahl von Netzwerkprotokollen und Ports. Die mitgelieferten Regelvorlagen erlauben es, die Grundeinstellungen einer Regel unter Berücksichtigung des Anwendungstyps schnell und bequem vorzunehmen.

Um auf der Basis einer Regelvorlage eine Regel für eine Anwendung zu erstellen,

1. Aktivieren Sie auf der Registerkarte **Regeln für Anwendungen** das Kontrollkästchen ☑ **Regeln nach Anwendungen ordnen**, wenn es deaktiviert war, und klicken Sie auf die Schaltfläche **Hinzufügen**.

2. Wählen Sie im folgenden Fenster die ausführbare Datei der Anwendung, für die die Regel erstellt werden soll. Dadurch wird die Regelliste für die gewählte Anwendung geöffnet. Wenn für sie bereits Regeln vorhanden sind, werden sie im oberen Bereich des Fensters angezeigt. Wenn keine Regeln vorhanden sind, ist das Regelfenster leer.

3. Klicken Sie im Fenster mit den Regeln der Anwendung auf die Schaltfläche **Vorlage** und wählen Sie aus dem Kontextmenü eine Regelvorlage (s. Abb. 46).

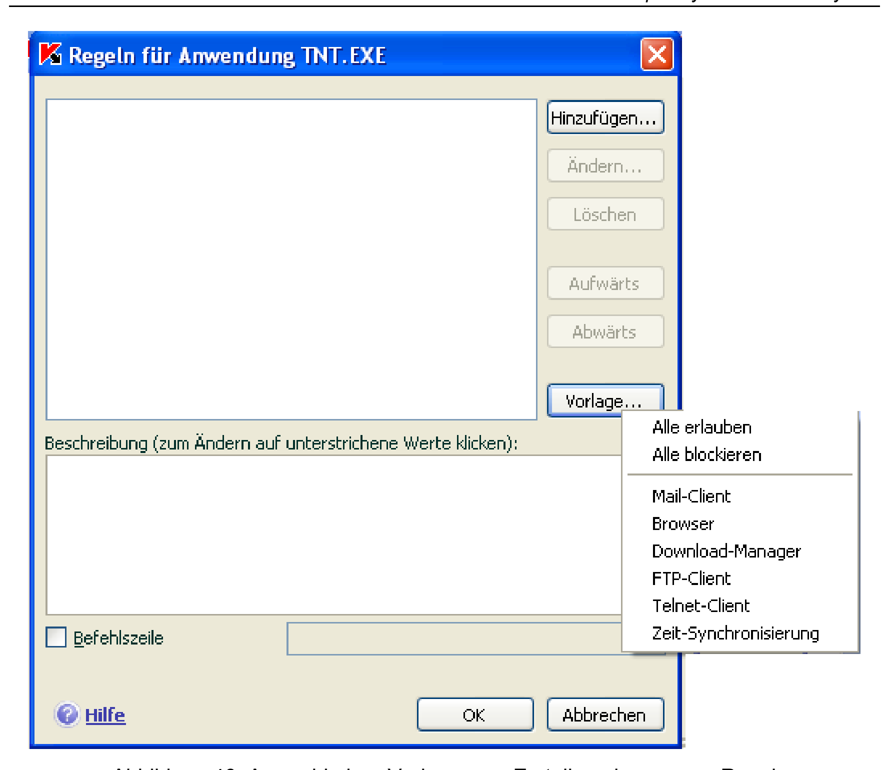


Abbildung 46. Auswahl einer Vorlage zum Erstellen einer neuen Regel

Alle erlauben ist eine Regel, die jede beliebige Netzwerkaktivität der Anwendung erlaubt. **Alle blockieren** ist eine Regel, die jede Netzwerkaktivität der Anwendung verbietet. Wenn für die Anwendung eine solche Verbotsregel vorhanden ist, werden alle Versuche der Anwendung, eine Netzwerkverbindung zu initiieren, ohne vorherige Benutzerbenachrichtigung blockiert.

Die übrigen Vorlagen, die im Kontextmenü vorhanden sind, erstellen eine Kombination von Regeln, die für die entsprechenden Programme charakteristisch sind. Die Vorlage **Mail-Client** erstellt beispielsweise eine Regelkombination, welche die für ein Mailprogramm standardmäßige Netzwerkaktivität wie das Senden von E-Mails erlaubt.

4. Korrigieren Sie bei Bedarf die für die Anwendung erstellten Regeln. Sie können die Aktion, die Richtung der Netzwerkverbindung, die Remoteadresse, die Ports (lokaler und entfernter Port) sowie die Gültigkeitsdauer der Regel ändern.

5. Wenn Sie möchten, dass die Regel für eine Anwendung gilt, die mit bestimmten Befehlszeilenparametern gestartet wird, dann aktivieren Sie das Kontrollkästchen ☑ **Befehlszeile** und nennen Sie im rechts angebrachten Feld die Zeile.

Die neue Regel wird am Ende der Liste hinzugefügt und erhält die niedrigste Priorität. Sie können die Ausführungspriorität der Regel ändern (s. Pkt. 12.4 auf S. 177).

Eine Regel kann auch aus dem Meldungsfenster über den Fund einer Netzwerkaktivität erstellt werden (s. Pkt. 12.10 auf S. 190).

12.3. Regeln für Pakete

Kaspersky Internet Security beinhaltet eine Auswahl von Regeln, die zur Filterung der durch Ihren Computer zu übertragenden und zu empfangenden Datenpakete dient. Die Paketübertragung kann von Ihnen oder von einer auf Ihrem Computer installierten Anwendung initiiert werden. Zum Lieferumfang des Programms gehören Filterregeln für Pakete, deren Übertragung von den Kaspersky-Lab-Spezialisten genau analysiert und nach strengen Maßstäben als gefährlich oder ungefährlich eingestuft wurden.

In Abhängigkeit von der Schutzstufe, die für die Arbeit der Firewall gewählt wurde, und dem Typ des Netzwerks, in dem der Computer arbeitet, wird die Regelliste auf unterschiedliche Weise verwendet. Auf der Stufe **Maximaler Schutz** wird beispielsweise jede Netzwerkaktivität, die nicht unter die Erlaubnisregeln fällt, blockiert.

Wichtiger Hinweis!

Beachten Sie, dass die Regeln für Sicherheitszonen eine höhere Priorität besitzen als die Verbotsregeln für Pakete. Bei Auswahl des Status **Lokales Netzwerk** wird beispielsweise der Austausch von Paketen sowie der Zugriff auf gemeinsame Ordner erlaubt, unabhängig davon, ob Verbotsregeln für Pakete vorhanden sind.

Zur Arbeit mit der Regelliste für Pakete:

1. Klicken Sie im Abschnitt Firewall des Konfigurationsfensters von Anti-Hacker auf die Schaltfläche **Einstellungen**.

2. Wählen Sie im folgenden Fenster die Registerkarte **Regeln für Pakete** (s. Abb. 47).

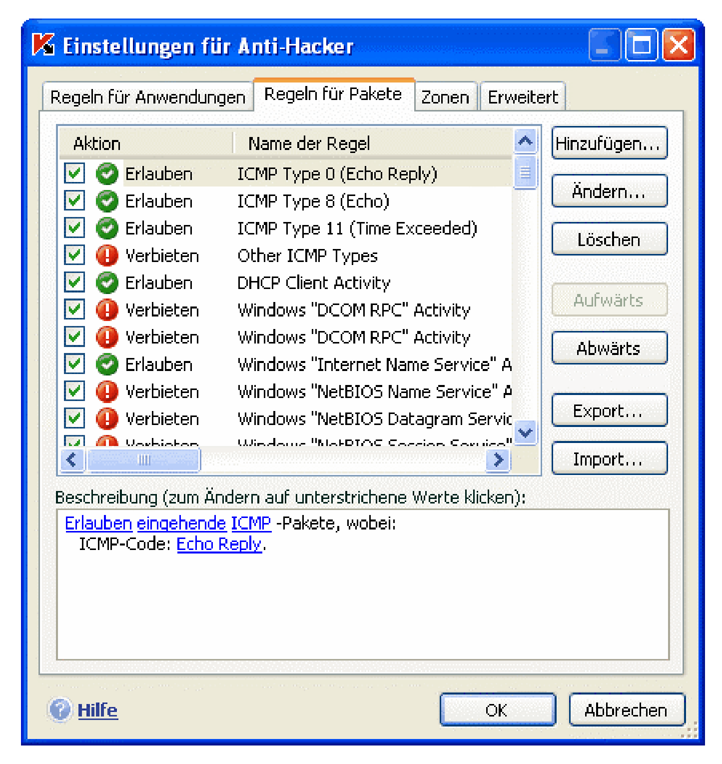


Abbildung 47. Liste der Regeln für die Paketfilterung

Für jede Filterregel sind folgende Informationen vorhanden: Name der Regel, Aktion (Erlaubnis oder Verbot der Paketübertragung), Protokoll zur Datenübertragung, Richtung des Pakets, sowie Parameter der Netzwerkverbindung, mit der die Paketübertragung ausgeführt wird.

Die Verwendung einer Filterregel wird durch das Kontrollkästchen neben ihrem Namen reguliert.

Die Arbeit mit der Regelliste erfolgt mit Hilfe der Schaltflächen, die sich rechts von der Liste befinden.

Um eine neue Paketregel zu erstellen,

> klicken Sie auf der Registerkarte **Regeln für Pakete** auf die **Schaltfläche Hinzufügen**.

Im folgenden Fenster **Neue Regel** kann die Regel erstellt und genau konfiguriert werden.

12.4. Detaillierte Konfiguration von Regeln für Anwendungen und Pakete

Das Fenster zum detaillierten Anpassen von Regeln (**Neue Regel**) ist für Anwendungen und Pakete praktisch identisch (S. Abbildung 48).

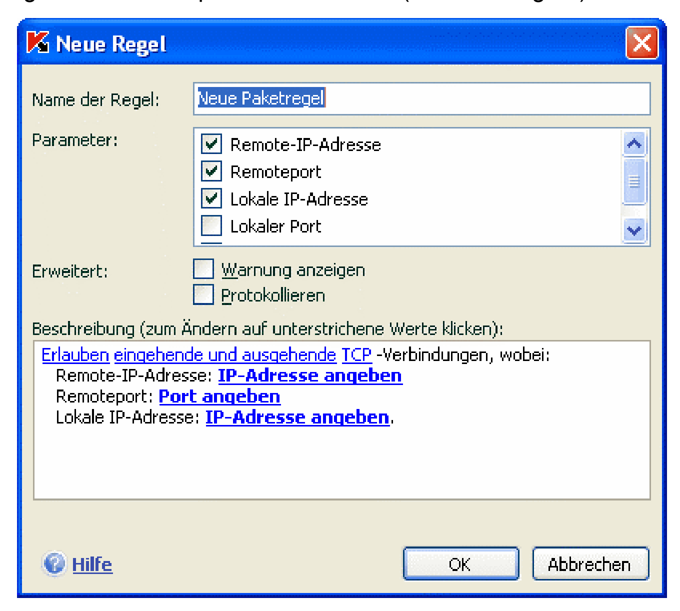


Abbildung 48. Erstellen einer neuen Regel für eine Anwendung

Der erste Schritt umfasst folgende Parameter:

- Der Name der Regel wird festgelegt. Das Programm verwendet einen standardmäßigen Namen, den Sie ändern können.
- Auswahl der Parameter für die Netzwerkverbindung, nach denen sich die Regel richten soll: Remoteadresse, Remoteport, lokale Adresse, lokaler Port und Gültigkeitsdauer der Regel. Aktivieren Sie die Kontrollkästchen der Parameter, die in der Regel verwendet werden sollen.
- Festlegen zusätzlicher Parameter, die der Benachrichtigung des Benutzers über die Verwendung der Regel dienen. Wenn Sie möchten, dass auf dem Bildschirm eine Popup-Meldung mit Kurzinformationen erscheint, wenn die Regel ausgeführt wird, aktivieren Sie das Kontroll-

kästchen ☑ **Warnung anzeigen**. Aktivieren Sie das Kontrollkästchen ☑ **Protokollieren**, damit Informationen über die Ausführung der Regel im Anti-Hacker-Bericht aufgezeichnet werden. Beim Erstellen einer Regel ist dieses Kontrollkästchen standardmäßig nicht aktiviert. Es wird empfohlen, die zusätzlichen Parameter beim Erstellen von Verbotsregeln zu verwenden.

> Beachten Sie, dass im Anti-Hacker-Trainingsmodus automatisch Informationen über eine Verbotsregel protokolliert werden, wenn die Regel verwendet wird. Falls das Aufzeichnen dieser Informationen nicht erforderlich ist, deaktivieren Sie das Kontrollkästchen **Protokollieren** in den Parametern der Regel.

Der zweite Schritt zum Erstellen einer Regel umfasst die Definition von Werten für die Parameter der Regel und die Auswahl einer Aktion. Diese Operationen erfolgen im Abschnitt **Beschreibung**.

1. Die Aktion einer erstellten Regel lautet *erlauben*. Um sie in eine Verbotsregel zu verwandeln, führen Sie im Beschreibungsabschnitt der Regel einen Linksklick auf den Link Erlauben aus. Er nimmt dadurch den Wert Verbieten an.

2. Wenn Sie vor dem Erstellen der Regel keine Anwendung gewählt haben, dann legen Sie diese jetzt mit dem Link Anwendung angeben fest. Klicken Sie mit der linken Maustaste auf den Link und wählen Sie im folgenden Standardfenster zur Dateiauswahl die ausführbare Datei der Anwendung, für welche die Regel erstellt wird.

3. Danach muss die Richtung der Netzwerkverbindung für die Regel bestimmt werden. Standardmäßig wird die Regel sowohl für eine eingehende als auch ausgehende Netzwerkverbindung erstellt. Um die Richtung zu ändern, klicken Sie mit der linken Maustaste auf den Link eingehende und ausgehende und wählen Sie im folgenden Fenster die Richtung der Netzwerkverbindung.

   - **Eingehender Strom**. Die Regel gilt für eine Netzwerkverbindung, die von einem entfernten Computer geöffnet wird.
   - **Eingehendes Paket**. Die Regel gilt für Datenpakete, die Ihr Computer empfängt, unter Ausnahme von TCP-Paketen.
   - **Eingehender und ausgehender Strom**. Die Regel gilt nur für eingehenden und ausgehenden Datenstrom, unabhängig davon, von welchem Computer (von Ihrem oder von einem entfernten) die Netzwerkverbindung initiiert wurde.
   - **Ausgehender Strom**. Die Regel gilt nur für eine Netzwerkverbindung, die von Ihrem Computer geöffnet wird.

Ausgehendes Paket. Die Regel gilt für Datenpakete, die von Ihrem Computer übertragen werden, unter Ausnahme von TCP-Paketen.

Wenn in der Regel die Richtung eines Pakets festgelegt werden soll, wählen Sie, ob es ein ausgehendes oder eingehendes Paket ist. Wenn Sie eine Regel für den Datenstrom erstellen möchten, wählen Sie den Typ des Datenstroms: eingehender, ausgehender oder beide Richtungen.

Der Unterschied zwischen der *Richtung des Datenstroms* und der *Richtung eines Pakets* besteht darin, dass beim Erstellen einer Regel für den Strom bestimmt wird, in welcher Richtung die Verbindung geöffnet wird. Die Richtung von Paketen bei der Datenübertragung für diese Verbindung wird nicht berücksichtigt.

Wenn Sie beispielsweise eine Regel für den Datenaustausch mit einem FTP-Server, der im passiven Modus arbeitet, konfigurieren, muss der ausgehende Strom erlaubt werden. Für den Datenaustausch mit einem FTP-Server, der im aktiven Modus arbeitet, muss sowohl der ausgehende als auch der eingehende Strom erlaubt werden.

4. Wenn als Parameter der Netzwerkverbindung die Remoteadresse gewählt wurde, klicken Sie mit der linken Maustaste auf den Link Adresse angeben und geben Sie im folgenden Fenster den Typ der IP-Adresse, einen Adressenbereich oder eine Subnetzadresse an. Für eine Regel können Sie einen oder mehrere IP-Adressentypen verwenden. Es können mehrere Adressen für jeden Typ festgelegt werden.

5. Bestimmen Sie dann das Protokoll, mit dem die Netzwerkverbindung ausgeführt werden soll. Als Standard wird eine Verbindung mit TCP-Protokoll verwendet. Beim Erstellen einer Regel für eine Anwendung kann zwischen den beiden Protokolltypen TCP und UDP gewählt werden. Klicken Sie dazu mit der linken Maustaste auf den Link mit dem Namen des Protokolls, bis er den gewünschten Wert annimmt. Wenn Sie eine Regel für ein Paket erstellen und den standardmäßigen Protokolltyp ändern möchten, klicken Sie auf den Link mit dem Protokollnamen und geben Sie im folgenden Fenster den erforderlichen Protokolltyp an. Bei Auswahl des ICMP-Protokolls kann zusätzlich die Angabe seines Typs erforderlich sein.

6. Wenn Sie Parameter für die Netzwerkverbindung gewählt haben (Adresse, Port, Gültigkeitsdauer der Regel), geben Sie genaue Werte dafür an.

Nachdem die Regel zur Regelliste für die Anwendung hinzugefügt wurde, können Sie zusätzliche Einstellungen vornehmen (s. Abbildung 49). Wenn Sie möchten, dass die Regel für eine Anwendung gilt, die mit bestimmten Befehlszeilenparametern gestartet wird, aktivieren Sie das Kontrollkästchen **Befehlszeile** und tragen Sie die Zeile im rechts angebrachten Feld ein. Für eine Anwendung, die mit einem anderen Befehlszeilenschlüssel gestartet wird, wird die Regel nicht ausgeführt.

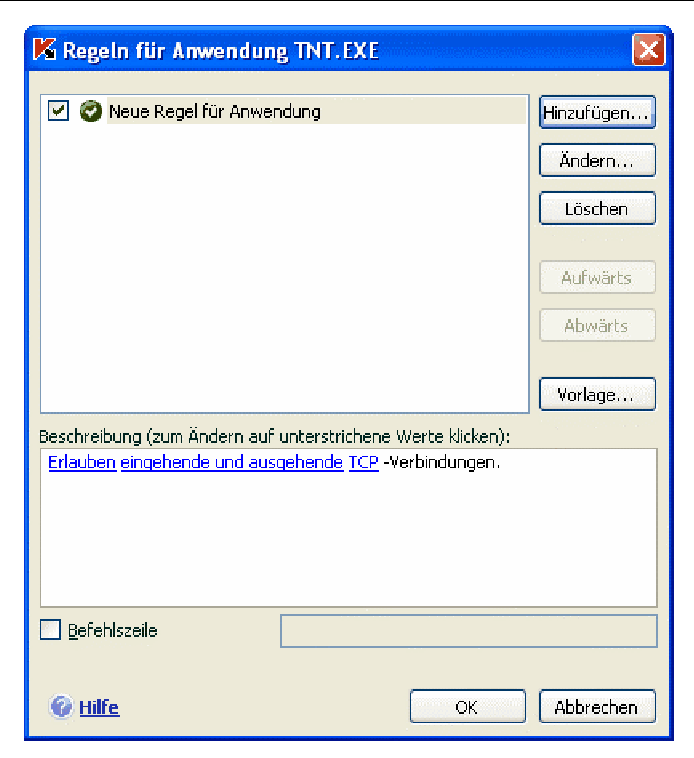


Abbildung 49. Erweiterte Einstellungen für eine neue Regel

Die Option zum Start der Anwendung mit bestimmten Befehlszeilenparametern steht für das Betriebssystem Microsoft Windows 98 nicht zur Verfügung.

Eine Regel kann auch aus dem Meldungsfenster über den Fund einer Netzwerkaktivität erstellt werden (s. Pkt. 12.10 auf S. 190).

12.5. Ändern der Priorität einer Regel

Jede Regel, die für eine Anwendung erstellt wurde, besitzt eine bestimmte Ausführungspriorität. Wenn die übrigen Bedingungen (beispielsweise die

Parameter der Netzwerkverbindung) übereinstimmen, wird für die Netzwerkaktivität der Anwendung jene Aktion verwendet, die von der Regel mit der höchsten Priorität bestimmt wird.

Die Priorität einer Regel wird durch ihre Position in der Regelliste bestimmt. Die erste Regel der Liste besitzt die höchste Ausführungspriorität. Jede manuell erstellte Regel wird am Anfang der Liste hinzugefügt. Regeln, die auf einer Vorlage basieren oder aus der speziellen Meldung erstellt wurden, werden am Ende der Regelliste hinzugefügt.

Um die Priorität einer Regel für eine Anwendung zu ändern, gehen Sie folgendermaßen vor:

1. Wählen Sie den Namen der Anwendung auf der Registerkarte **Regeln für Anwendungen**.
2. Verwenden Sie im folgenden Fenster mit den für die Anwendung erstellten Regeln die Schaltflächen **Aufwärts** und **Abwärts**, um die Position der Regeln in der Liste und dementsprechend ihre Priorität zu verändern.

Um die Priorität einer Regel für ein Paket zu ändern, gehen Sie folgendermaßen vor:

1. Wählen Sie die Regel auf der Registerkarte **Regeln für Pakete**.
2. Verwenden Sie im folgenden Fenster mit den Paketregeln die Schaltflächen **Aufwärts** und **Abwärts**, um die Position der Regeln in der Liste und dementsprechend ihre Priorität zu verändern.

12.6. Regeln für Sicherheitszonen

Nach der Installation analysiert Anti-Hacker die Netzwerkumgebung Ihres Computers. Aufgrund der Analyseergebnisse wird die gesamte Netzwerkumgebung in bedingte Zonen unterteilt:

Internet – globales Netzwerk Internet. In dieser Zone arbeitet Kaspersky Internet Security als Personal Firewall. Dabei wird die gesamte Netzwerkaktivität durch Regeln für Pakete und Anwendungen geregelt, die in der Grundeinstellung maximale Sicherheit gewährleisten. Die Schutzbedingungen bei der Arbeit in dieser Zone können nicht geändert werden. Zur Steigerung der Sicherheit kann der Stealth-Modus aktiviert werden.

Sicherheitszonen – verschiedene bedingte Zonen, die teilweise mit Subnetzen übereinstimmen, zu denen der Computer gehört (auch lokale Netzwerke zu Hause oder bei der Arbeit). Diese Zonen werden standardmäßig als Zonen mit mittlerer Risikostufe betrachtet. Sie können den Status dieser Zonen in Abhängigkeit der

Vertrauenswürdigkeit des jeweiligen Subnetzes ändern, sowie die Regeln für Pakete und Anwendung anpassen.

Wenn der Trainingsmodus aktiviert ist, zeigt Anti-Hacker bei jeder Verbindung des Computers zu einer neuen Zone ein Fenster an, das eine kurze Beschreibung der Zone enthält. Es ist Ihre Aufgabe, dieser Zone einen Status zuzuweisen, auf dessen Grundlage die jeweilige Netzwerkaktivität erlaubt oder verboten wird:

- **Internet**. Dieser Status wird standardmäßig dem Internet zugeordnet, weil der Computer bei der Arbeit im Internet allen möglichen Typen von Bedrohungen unterliegt. Die Auswahl dieses Status wird außerdem für Netzwerke empfohlen, die nicht durch Antiviren-Anwendungen, Firewalls, Filter usw. geschützt werden. Bei der Auswahl dieses Status wird die maximale Sicherheit der Arbeit des Computers in dieser Zone gewährleistet. Das bedeutet:

    - Jede beliebige netzwerkbezogene NetBios-Aktivität im Rahmen des Subnetzes wird blockiert.

    - Das Ausführen von Regeln für Anwendungen und Pakete, die eine netzwerkbezogene NetBios-Aktivität im Rahmen dieses Subnetzes erlauben, wird verboten.

  Selbst wenn Sie einen gemeinsamen Ordner erstellt haben, besitzen die Benutzer eines Subnetzes mit diesem Status keinen Zugriff auf die darin enthaltenen Informationen. Außerdem haben Sie bei Auswahl dieses Status keinen Zugriff auf Dateien und Drucker auf anderen Computern des Netzwerks.

- **Lokales Netzwerk**. Dieser Status wird standardmäßig der Mehrzahl der Sicherheitszonen zugewiesen, die bei der Analyse der Netzwerkumgebung des Computers gefunden werden. Eine Ausnahme bildet das Internet. Es wird empfohlen, diesen Status für Zonen mit mittlerer Risikostufe zu verwenden (beispielsweise für ein lokales Firmennetzwerk). Bei der Auswahl dieses Status wird erlaubt:

    - jede beliebige netzwerkbezogene NetBios-Aktivität im Rahmen des Subnetzes.

    - das Ausführen von Regeln für Anwendungen und Pakete, die eine netzwerkbezogene NetBios-Aktivität im Rahmen dieses Subnetzes erlauben.

  Wählen Sie diesen Status, wenn Sie Zugriff auf bestimmte Verzeichnisse oder Drucker Ihres Computers gewähren, aber jede andere externe Aktivität verbieten möchten.

- **Vertrauenswürdig**. Es wird empfohlen, diesen Status nur für eine Zone zu verwenden, die Ihrer Meinung nach absolut sicher ist und in welcher

dem Computer bei der Arbeit weder Angriffe noch Versuche zu unerlaubtem Datenzugriff drohen. Bei der Auswahl dieses Status wird jede beliebige Netzwerkaktivität erlaubt. Selbst wenn Sie die Stufe Maximaler Schutz gewählt und Verbotsregeln erstellt haben, gelten diese nicht für entfernte Computer eines vertrauenswürdigen Netzwerks.

Beachten Sie, dass jede Zugriffsbegrenzung für die Arbeit mit Dateien nur im Rahmen des jeweiligen Subnetzes wirksam ist.

Für ein Netzwerk mit dem Status **Internet** können Sie zur Erhöhung der Sicherheit den Stealth-Modus verwenden. In diesem Modus wird nur die Netzwerkaktivität erlaubt, die von Ihrem Computer initiiert wurde. Praktisch bedeutet das, dass Ihr Computer für die externe Umgebung "unsichtbar" wird. Gleichzeitig beeinträchtigt der Modus aber Ihre Arbeit im Internet in keiner Weise.

Es wird davor gewarnt, den Stealth-Modus zu verwenden, wenn der Computer als Server dient (beispielsweise als Mailserver oder http-Server). Andernfalls können Computer, die sich an den Server wenden, diesen im Netzwerk nicht finden.

Eine Liste der Zonen, in denen Ihr Computer angemeldet war, befindet sich auf der Registerkarte **Zonen** (s. Abb. 50). Für jede Zone werden der Status und eine kurze Beschreibung des Netzwerks angegeben. Außerdem wird darüber informiert, ob der Stealth-Modus verwendet wird oder nicht.

Um den Status einer Zone zu ändern oder den Stealth-Modus zu aktivieren bzw. deaktivieren, wählen Sie die Zone in der Liste aus und verwenden Sie die entsprechenden Links im Block **Beschreibung**, der sich unterhalb der Liste befindet. Diese Aktionen können auch im Fenster **Parameter der Zone** vorgenommen werden, das mit der Schaltfläche **Ändern** geöffnet wird. In diesem Fenster können auch Adresse und Maske des Subnetzes geändert werden.

Unter Verwendung der Schaltfläche **Suchen** können Sie der Liste eine neue Zone hinzufügen. In diesem Fall sucht Anti-Hacker nach Zonen, in denen die Anmeldung möglich ist. Wenn solche Zonen gefunden werden, wird Ihnen angeboten, deren Status festzulegen. Daneben können Sie einen neue Zone auch manuell zur Liste hinzufügen (beispielsweise wenn Sie ein Notebook an ein neues Netzwerk anschließen). Verwenden Sie dazu die Schaltfläche **Hinzufügen** und geben Sie im Fenster **Parameter der Zone** die erforderlichen Informationen an.

Um ein Netzwerk aus der Liste zu löschen, verwenden Sie die Schaltfläche **Löschen**.

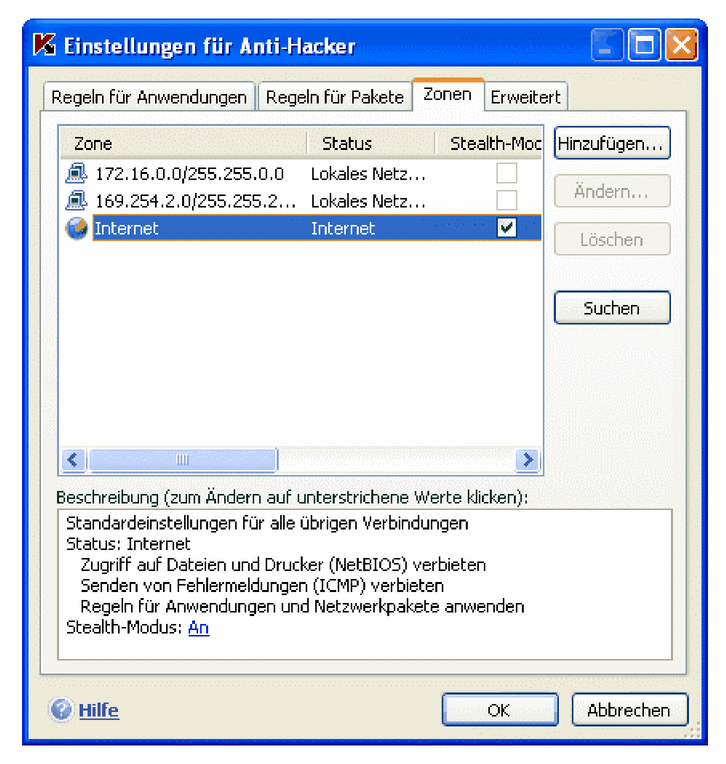


Abbildung 50. Liste der Regeln für Zonen

12.7. Funktionsmodus der Firewall

Der Modus für die Arbeit der Firewall (s. Abbildung 51) reguliert die Kompatibilität von Anti-Hacker mit Programmen, die mehrfache Netzwerkverbindungen herstellen, und mit Netzwerkspielen.

Maximale Kompatibilität – Dieser Funktionsmodus der Firewall gewährleistet die optimale Arbeit für die Komponente Anti-Hacker und Programme, die mehrfache Netzwerkverbindungen aufbauen (Clients zum Dateiaustausch über Netzwerke). Allerdings kann dieser Modus in bestimmten Fällen zu erhöhter Reaktionszeit in Netzwerkspielen führen. Sollte diese Situation eintreten, wird die Verwendung des Modus Maximales Tempo empfohlen.

Maximales Tempo – Dieser Funktionsmodus der Firewall gewährleistet die maximale Reaktionsgeschwindigkeit in Netzwerkspielen. Allerdings sind in diesem Modus Konflikte bei der Arbeit von Clients zum Dateiaustausch über

Netzwerke und anderer Netzwerkanwendungen möglich. Zur Lösung des Problems wird empfohlen, den Stealth-Modus zu deaktivieren.

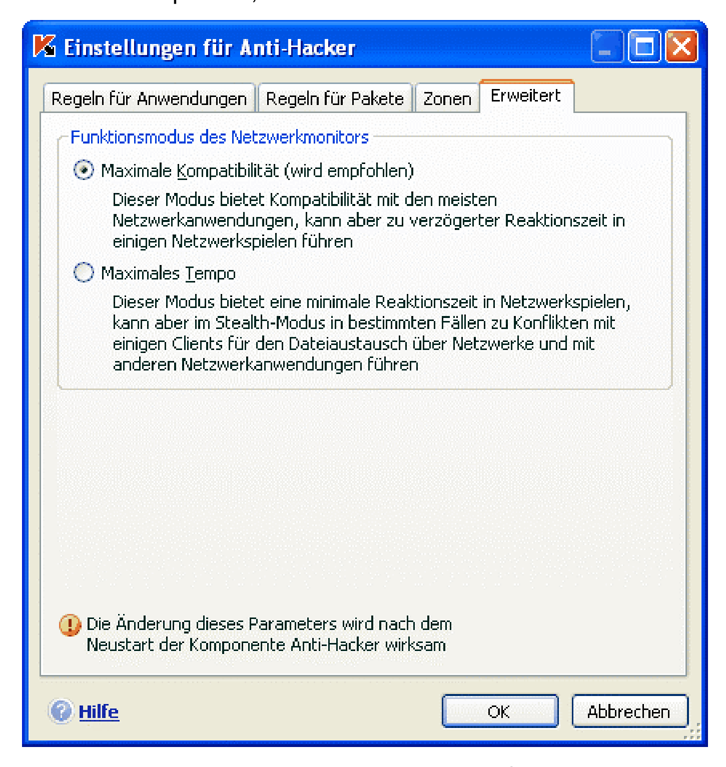


Abbildung 51. Auswahl des Funktionsmodus für Anti-Hacker

Um den Firewall-Funktionsmodus anzupassen,

1. Klicken Sie auf die Schaltfläche **Einstellungen** im Abschnitt **Allgemein** des Konfigurationsfensters von Anti-Hacker.

2. Gehen Sie im folgenden Fenster auf die Registerkarte **Erweitert** und wählen Sie den gewünschten Funktionsmodus: Maximale Kompatibilität oder Maximales Tempo.

Das Ändern des Funktionsmodus für den Netzwerkmonitor wird erst nach dem Neustart der Komponente Anti-Hacker wirksam.

12.8. Konfiguration des Detektionssystems für Angriffe

Alle momentan bekannten Netzwerkangriffe, von denen der Computer bedroht werden kann, sind in den Bedrohungssignaturen enthalten. Auf der Basis einer Liste dieser Angriffe arbeitet das **Detektionsmodul für Angriffe** der Komponente Anti-Hacker. Die Liste der Angriffe, die von diesem Modul erkannt werden können, wird beim Update der Signaturen ergänzt (s. Kapitel 15 auf S. 237). In der Grundeinstellung aktualisiert Kaspersky Internet Security die Angriffssignaturen nicht.

Das Detektionssystem für Angriffe überwacht die Netzwerkaktivität, die für Netzwerkangriffe typisch ist. Wenn er einen Angriffsversuch auf Ihren Computer registriert, blockiert er jede beliebige Art von Netzwerkaktivität des angreifenden Computers im Hinblick auf Ihrem Computer für eine Stunde. Auf dem Bildschirm erscheint eine Meldung darüber, dass ein Netzwerkangriff versucht wurde. Die Meldung enthält Informationen über den angreifenden Computer.

Die Arbeit des Detektionssystems für Angriffe lässt sich folgendermaßen konfigurieren:

1. Öffnen Sie das Konfigurationsfenster von Anti-Hacker.

2. Klicken Sie im Abschnitt **Detektionssystem für Angriffe** auf die Schaltfläche **Einstellungen**.

3. Legen Sie im folgenden Fenster (s. Abb. 52) fest, ob ein angreifender Computer blockiert werden soll, und wenn ja, für welchen Zeitraum. Standardmäßig wird ein angreifender Computer für 60 Minuten blockiert. Sie können die Sperrzeit verkürzen oder verlängern, indem Sie den Wert im Feld neben dem Kontrollkästchen ☑ **Angreifenden Computer blockieren für ... Min.** ändern. Wenn die Netzwerkaktivität des angreifenden Computers im Hinblick auf Ihren Computer nicht blockiert werden soll, deaktivieren Sie das Kontrollkästchen.



Abbildung 52. Anpassen des Zeitraums für den ein angreifender Computer blockiert werden soll

12.9. Liste der erkennbaren Netzwerkangriffe

Heutzutage existiert einen Vielzahl unterschiedlicher Arten von Netzwerkangriffen, die sowohl Schwachstellen des Betriebssystems, als auch installierter System- und Anwendungsprogramme benutzen. Die Angreifer vervollkommnen ihre Methoden ständig und die Folgen eines Angriffs können im Diebstahl vertraulicher Informationen, Systemabsturz oder vollständiger Übernahme des Systems mit späterer Verwendung als Teil eines Zombie-Netzwerks für neue Angriffe bestehen.

Um rechtzeitig für die Sicherheit eines Computers zu sorgen, ist es wichtig zu wissen, welche Arten von Netzwerkangriffen ihm drohen können. Die bekannten Netzwerkbedrohungen lassen sich bedingt in drei große Gruppen unterteilen:

- **Scannen von Ports** – Diese Art der Bedrohung stellt eigentlich keinen Angriff dar, sondern geht diesem voraus, weil sie eine der effektivsten Methoden ist, Informationen über einen entfernten Computer zu erhalten. Diese Methode besteht darin, die von Netzwerkdiensten auf dem angegriffenen Computer verwendeten UDP/TCP-Ports zu scannen, um deren Status (geschlossene oder offene Ports) zu ermitteln.

  Das Scannen von Ports gibt Aufschluss darüber, welche Angriffstypen für ein bestimmtes System am meisten Erfolg versprechen. Außerdem verleihen die aus dem Scannen resultierenden Informationen ("Abdruck" des Systems) dem Angreifer eine Vorstellung vom Typ des Betriebssystems auf dem entfernten Computer. Dadurch lässt sich die Art der passenden Angriffe weiter einkreisen und damit die zum Ausführen der Angriffe notwendige Zeit verkürzen. Außerdem können die für das Betriebssystem spezifischen Sicherheitslücken ausgenutzt werden.

- **DoS-Angriffe (Denial of Service = Verweigerung des Diensts)** – Das Ziel dieser Angriffe besteht darin, die Instabilität des angegriffenen Systems hervorzurufen oder es vollständig außer Gefecht zu setzen. Die Folgen dieses Angriffstyps können Beschädigung oder Zerstörung der angegriffenen Informationsressourcen sein, die dadurch unzugänglich werden.

  Es gibt zwei Haupttypen von DoS-Angriffen:

  - Es werden spezielle Pakete an den angegriffenen Computer geschickt, die dieser nicht erwartet. Die Folge ist eine Überlastung oder Systemabsturz.
  - An den angegriffenen Computer wird innerhalb eines kurzen Zeitraums eine hohe Anzahl von Paketen geschickt, die dieser

Computer nicht verarbeiten kann. In der Folge erschöpfen die Systemressourcen.

Die folgenden Angriffe bieten gute Beispiele für diese Gruppe:

- Der Angriff *Ping of death* besteht im Senden eines ICMP-Pakets, dessen Größe den zulässigen Wert von 64 KB überschreitet. Dieser Angriff kann zum Absturz bestimmter Betriebssysteme führen.
- Bei dem Angriff *Land* wird an einen offenen Port Ihres Computers eine Anfrage auf Verbindungsherstellung mit sich selbst gesendet. Der Angriff führt zu einer Endlosschleife im angegriffenen Computer, was eine stark erhöhte Prozessorbelastung zur Folge hat und bei bestimmten Betriebssystemen zum Absturz führen kann.
- Bei dem Angriff *ICMP Flood* wird eine hohe Anzahl von ICMP-Paketen an Ihren Computer gesendet. Da der Computer auf jedes eintreffende Paket reagieren muss, erhöht sich die Prozessorbelastung stark.
- Bei dem Angriff *SYN Flood* wird eine große Menge von Verbindungsanfragen an Ihren Computer gesendet. Das System reserviert für jede dieser Verbindungen bestimmte Ressourcen, wodurch es seine gesamten Ressourcen verbraucht und nicht mehr auf andere Verbindungsversuche reagiert.

- **Angriffe zur "Übernahme"** – Diese Angriffe zielen auf die "Übernahme" des Systems ab. Es ist der gefährlichste Angriffstyp, weil das System bei erfolgreichem Angriff dem Angreifer gegenüber vollkommen wehrlos ist.

  Dieser Angriff wird benutzt, um vertrauliche Informationen von einem entfernten Computer zu erhalten (beispielsweise Kreditkartennummern und Kennwörter). Ein weiteres Ziel kann darin bestehen, sich im System einzunisten, um später die Rechnerressourcen zu Zwecken des Angreifers zu benutzen (das angegriffene System wird in einem Zombie-Netzwerk oder als "Brückenkopf" für neue Angriffe verwendet).

  Diese Gruppe ist am umfangreichsten und lässt sich abhängig vom Betriebssystem in drei Untergruppen aufteilen: Angriffe unter Microsoft Windows, Angriffe unter Unix und eine allgemeine Gruppe für Netzwerkdienste, die in beiden Betriebssystemen verwendet wird.

  Die meistverbreiteten Arten von Angriffen, welche die Netzwerkdienste eines Betriebssystems verwenden, sind:

  - *Angriffe mit dem Ziel des Pufferüberlaufs* – Eine Schwachstelle in Programmen, die aufgrund der fehlenden (oder

unzureichenden) Kontrolle bei der Arbeit mit großen Datenmengen entsteht. Dieser Typ von Schwachstellen gehört zu den ältesten und lässt sich am leichtesten von Angreifern ausnutzen.

- *Formatstring-Angriffe* beruhen auf Fehlern in Formatzeilen. Ein Schwachstellentyp in Programmen, der darauf beruht, dass die Eingabeparameter von Formatfunktionen des Typs printf(), fprintf(), scanf() und anderer Standardbibliotheken der Sprache C unzureichend kontrolliert werden. Wenn diese Sicherheitslücke in einem Programm vorhanden ist, kann ein bösartiger Benutzer die vollständige Kontrolle über das System ergreifen, wenn er die Möglichkeit besitzt, speziell erstellte Anfragen zu senden.

Das Detektionssystem für Angriffe analysiert und verhindert solche Sicherheitslücken in den gebräuchlichsten Netzwerkdiensten (FTP, POP3, IMAP) automatisch, wenn sie auf dem Computer verwendet werden.

Angriffe, die das Betriebssystem Microsoft Windows betreffen, beruhen auf der Verwendung von Sicherheitslücken der auf dem Computer installierten Software (beispielsweise solcher Programme wie Microsoft SQL Server, Microsoft Internet Explorer, Messenger, sowie Systemkomponenten, die über ein Netzwerk erreichbar sind: DCom, SMB, Wins, LSASS, IIS5).

Die Komponente Anti-Hacker schützt den Computer beispielsweise vor Angriffen, die die folgenden bekannten Sicherheitslücken von Programmen missbrauchen (die Liste der Sicherheitslücken entspricht der Nummerierung der Microsoft Knowledge Base):

(**MS03-026**) DCOM RPC Vulnerability(Lovesan worm)

(**MS03-043**) Microsoft Messenger Service Buffer Overrun

(**MS03-051**) Microsoft Office Frontpage 2000 Server Extensions Buffer Overflow

(**MS04-007**) Microsoft Windows ASN.1 Vulnerability

(**MS04-031**) Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow

(**MS04-032**) Microsoft Windows XP Metafile (.emf) Heap Overflow

(**MS05-011**) Microsoft Windows SMB Client Transaction Response Handling

(**MS05-017**) Microsoft Windows Message Queuing Buffer Overflow Vulnerability

(**MS05-039**) Microsoft Windows Plug-and-Play Service Remote Overflow

(**MS04-045**) Microsoft Windows Internet Naming Service (WINS) Remote Heap Overflow

(**MS05-051**) Microsoft Windows Distributed Transaction Coordinator Memory Modification

Ein weiterer häufig anzutreffender Angriffstyp, der die Übernahme des Systems verfolgt, ist die Verwendung unterschiedlicher Arten von schädlichen Skripte, wozu auch Skripte gehören, die von Microsoft Internet Explorer verarbeitet werden, sowie die Variationen des Wurms Helkern. Bei dem Angriff *Helkern* werden spezielle UDP-Pakete mit ausführbarem schädlichem Code an den entfernten Computer gesendet.

Denken Sie daran, dass Ihr Computer bei der Arbeit in einem Netzwerk ständig dem Risiko eines Angriffs durch böswillige Benutzer ausgesetzt ist. Um die Sicherheit des Computers zu gewährleisten, aktivieren Sie bei der Arbeit im Internet unbedingt die Komponente Anti-Hacker und aktualisieren Sie die Signaturen für Hackerangriffe (s. Pkt. 16.4.2 auf S. 249).

12.10. Erlauben/Verbieten der Netzwerkaktivität

Wenn als Schutzstufe für die Firewall der **Trainingsmodus** gewählt wurde, wird jedes Mal, wenn versucht wird, eine Netzwerkverbindung auszuführen, für die keine Regel vorhanden ist, eine spezielle Meldung (s. Abb.) auf dem Bildschirm angezeigt.

Wenn Sie für die Arbeit mit elektronischer Post beispielsweise Microsoft Office Outlook verwenden, lädt das Mailprogramm nach dem Öffnen Ihre E-Mails von einem entfernten Exchange-Server. Um Ihre Mailbox zu erreichen, führt das Programm eine Netzwerkverbindung mit dem Mailserver aus. Eine solche Netzwerkaktivität wird von Anti-Hacker standardmäßig verfolgt. In diesem Fall wird eine Meldung (s. Abb. 53) mit folgendem Inhalt angezeigt:

- *Beschränkung der Aktivität* – Name der Anwendung und Kurzcharakteristik der Verbindung, die von ihr initiiert wurde. In der Regel werden folgende Daten angezeigt: Verbindungstyp, lokaler Port, von dem aus sie initiiert wurde, Remoteport und Adresse, mit der die Verbindung ausgeführt wurde. Führen Sie an einer beliebigen Stelle des Beschreibungsblocks einen Linksklick aus, um ausführlichere Informationen über die Netzwerkaktivität zu erhalten. Im folgenden Fenster werden Informationen über die Verbindung, den Prozess, der sie initiiert und über den Hersteller der Anwendung angezeigt.

- *Aktion* – Reihenfolge der Operationen, die von Anti-Hacker mit der erkannten Netzwerkaktivität ausgeführt werden soll. Genau in diesem Punkt ist Ihre Entscheidung erforderlich.

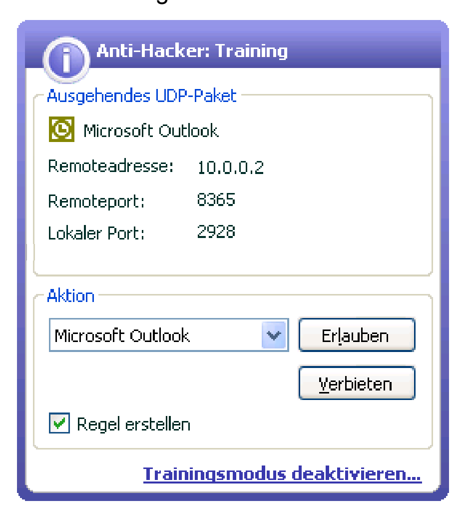


Abbildung 53. Meldung über Netzwerkaktivität

Lesen Sie aufmerksam die Informationen über die Netzwerkaktivität und wählen Sie dann die Aktion für Anti-Hacker. Wir empfehlen Ihnen, bei Ihrer Entscheidung folgende Ratschläge zu berücksichtigen:

1. Entscheiden Sie zuerst, ob die Netzwerkaktivität erlaubt oder verboten wird. Möglicherweise ist Ihnen in diesem Fall die Sammlung der Regeln behilflich, die bereits für die Anwendung oder für das Paket erstellt worden sind (unter der Voraussetzung, dass solche Regeln vorhanden sind). Verwenden Sie dazu den Link **Vorhandene Regeln**. Dadurch wird ein Fenster mit einer vollständigen Liste der Regeln geöffnet, die für die Anwendung oder das Datenpaket erstellt worden sind.

2. Bestimmen Sie danach, ob die Aktion nur einmal oder jedes Mal automatisch beim Fund dieser Aktivität ausgeführt werden soll.

Damit die Aktion nur einmal ausgeführt wird,

deaktivieren Sie das Kontrollkästchen ☑ **Regel erstellen** und klicken Sie auf die Schaltfläche mit dem Namen der Aktion, beispielsweise auf die Schaltfläche **Erlauben**.

Damit die von Ihnen gewählte Aktion automatisch ausgeführt wird, wenn diese Aktivität auf Ihrem Computer initiiert wird,

1. Aktivieren Sie das Kontrollkästchen ☑ **Regel erstellen**.

2. Wählen Sie den Typ der Aktivität, auf welche die Aktion angewandt werden soll, aus der Dropdown-Liste des Blocks **Aktion**:

   - **Jede Aktivität** – Netzwerkaktivität beliebigen Charakters, die von dieser Anwendung initiiert wird.
   - **Benutzerdefiniert** – eine einzelne Aktivität, die von Ihnen in einem speziellen Fenster festgelegt werden muss. Der Vorgang entspricht dem Erstellen einer Regel (s. Pkt. 12.2.1 auf S. 172).
   - **<Vorlage>** – Name einer Vorlage, die zur Sammlung der Regeln gehört, die für die Netzwerkaktivität der Anwendung charakteristisch sind. Dieser Aktivitätstyp erscheint dann in der Liste, wenn für die Anwendung, welche die Netzwerkaktivität initiiert hat, im Lieferumfang von Kaspersky Internet Security eine passende Vorlage vorhanden ist (s. Pkt. 12.2.2 auf S. 173). Verwenden Sie die Vorlage und erstellen Sie auf diese Weise automatisch eine Regelkombination für die Anwendung.

3. Klicken Sie auf die Schaltfläche mit dem Namen der Aktion (**Erlauben** oder **Verbieten**).

Beachten Sie, dass die erstellte Regel nur dann verwendet wird, wenn alle Verbindungsparameter erfüllt werden. Für eine Verbindung, die beispielsweise von einem anderen lokalen Port aus erfolgt, ist diese Regel ungültig.

KAPITEL 13. SCHUTZ VOR UNERWÜNSCHTEN E-MAILS

Kaspersky Internet Security 6.0 besitzt eine spezielle Komponente, die es erlaubt, unerwünschte E-Mails (Spam) zu erkennen und sie nach den Regeln Ihres Mailprogramms zu bearbeiten. Dadurch sparen Sie bei der Arbeit mit elektronischer Post viel Zeit.

Die Spam-Untersuchung von E-Mail-Nachrichten erfolgt nach folgendem Algorithmus:

1. Es wird geprüft, ob die Absenderadresse der E-Mail-Nachricht in der schwarzen oder weißen Adressenliste enthalten ist.
   - Wenn sich die Absenderadresse in der weißen Liste befindet, erhält der Brief den Status *Kein Spam*.
   - Wenn sich die Absenderadresse in der schwarzen Liste befindet, erhält die Nachricht den Status *Spam*. Die weitere Bearbeitung ist von der durch Sie ausgewählten Aktion abhängig (s. Pkt. 13.3.8 auf S. 212).
2. Wenn die Absenderadresse nicht in der schwarzen oder weißen Liste gefunden wird, wird die E-Mail mit Hilfe der PDB-Technologie (s. Pkt. 13.3.2 auf S. 202) auf das Vorhandensein von Spam-Phrasen analysiert. Die Analyse basiert auf der Datenbank, die beim Anti-Spam-Training erstellt wurde.
3. Anti-Spam analysiert den E-Mail-Text ausführlich und untersucht ihn auf das Vorhandensein von Wörtern aus der schwarzen und weißen Liste.
   - Wenn der Nachrichtentext eine Zeile aus der weißen Wörterliste enthält, erhält der Brief den Status *KEIN Spam*.
   - Wenn im Text eine Zeile aus der schwarzen Wörterliste gefunden wird, erhält die Nachricht den Status *Spam*. Die weitere Bearbeitung der Nachricht ist von der ausgewählten Aktion abhängig.
4. Wenn die E-Mail-Nachricht keine Zeilen aus der schwarzen und weißen Liste enthält, wird eine Phishing-Analyse ausgeführt. Wenn der Nachrichtentext eine Adresse enthält, die in der Anti-Phishing-Datenbank enthalten ist, erhält die Nachricht den Status *Spam*. Die weitere Bearbeitung der Nachricht ist von der ausgewählten Aktion abhängig.

5. Wenn die Nachricht keine Phishing-Zeilen enthält, erfolgt die Spam-Analyse mit Hilfe spezieller Technologien:

   - Grafikanalyse mit der GSG-Technologie
   - Analyse des Nachrichtentexts unter Verwendung des Spam-Analysealgorithmus – iBayes-Algorithmus.

6. Danach erfolgt die Untersuchung von zusätzlichen Merkmalen der Spam-Filterung (s. Pkt. 13.3.5 auf S. 209), die vom Benutzer bei der Konfiguration von Anti-Spam festgelegt wurden. Dazu zählen u.a. Überprüfung der Korrektheit von HTML-Tags, Schriftgröße und unsichtbaren Zeichen.

Jede der oben beschriebenen Etappen, die eine Nachricht bei der Spam-Analyse durchläuft, kann deaktiviert werden.

Anti-Spam wird als Erweiterungsmodul in folgende Mailprogramme integriert:

- Microsoft Office Outlook (s. Pkt. 13.3.9 auf S. 213)
- Microsoft Outlook Express (s. Pkt. 13.3.10 auf S. 217)
- The Bat! (s. Pkt. 13.3.11 auf S. 218)

In dieser Version von Kaspersky Internet Security sind keine Anti-Spam-Erweiterungsmodule für die 64-Bit-Versionen der Mailprogramme Microsoft Office Outlook, Microsoft Outlook Express und The Bat! vorgesehen.

In der Symbolleiste der Mailprogramme Microsoft Office Outlook und Microsoft Outlook Express finden Sie die beiden Schaltflächen **Spam** und **Kein Spam**, die dazu dienen, Anti-Spam für das Erkennen unerwünschter Post in Ihrer Korrespondenz zu konfigurieren. In The Bat! fehlen solche Schaltflächen, dafür kann das Training mit Hilfe der speziellen Punkte **Als Spam markieren** und **Als KEIN Spam markieren** im Menü **Extras** erfolgen. Außerdem werden allen Parametern des Mailprogramms spezielle Parameter zur Bearbeitung unerwünschter E-Mail-Korrespondenz hinzugefügt (s. Pkt. 13.3.1 auf S. 201).

Anti-Spam verwendet einen modifizierten lernfähigen Bayes-Algorithmus, was der Komponente erlaubt, mit der Zeit genauer zwischen *Spam* und *nützlicher Post* zu unterscheiden.

Es kann sein, dass der modifizierte iBayes-Algorithmus nicht fähig ist, eine bestimmte E-Mail-Nachricht mit hoher Wahrscheinlichkeit als Spam oder nützliche Post zu klassifizieren. Eine solche Nachricht erhält den Status *Potentieller Spam*.

Um die Anzahl der E-Mail-Nachrichten zu verringern, die als potentieller Spam gelten, wird empfohlen, mit solchen Briefen ein zusätzliches Anti-Spam-Training

durchzuführen (s. Pkt. 13.2 auf S. 197). Dazu muss festgelegt werden, welche dieser Briefe *Spam* und welche *KEIN Spam* sind.

E-Mail-Nachrichten, die als *Spam* oder *Potentieller Spam* gelten, werden modifiziert: Im Feld **Betreff** der Nachricht wird die Markierung **[!! SPAM]** bzw. **[?? Probable Spam]** hinzugefügt.

Die Bearbeitungsregeln für E-Mail-Nachrichten, die als Spam oder potentieller Spam markiert wurden, werden für die Mailprogramme Microsoft Office Outlook, Microsoft Outlook Express und The Bat! in den speziellen Erweiterungsmodulen festgelegt, die für diese Programme entwickelt wurden. Für andere Mailprogramme können Sie Filterregeln einstellen, damit sie das Feld **Betreff** der Nachricht beachten und eine E-Mail-Nachricht beispielsweise in Abhängigkeit davon, ob darin die Markierung **[!! SPAM]** oder **[?? Probable Spam]** vorhanden ist, in einen entsprechenden Ordner verschieben. Eine ausführlichere Beschreibung des Filtermechanismus finden Sie in der Dokumentation Ihres Mailprogramms.

13.1. Auswahl der Anti-Spam-Aggressivitätsstufe

Kaspersky Internet Security bietet den Spam-Schutz auf einer der folgenden Stufen (s. Abb. 54):

Alle blockieren – Höchste Aggressivitätsstufe, auf der alle E-Mails als Spam klassifiziert werden, außer Nachrichten, die Zeilen aus der weißen Wörterliste und Absender, die in der weißen Liste genannt sind, enthalten (s. Pkt. 13.3.4.1 auf S. 205). Auf dieser Stufe erfolgt die Briefanalyse nur mit der weißen Liste, die Verwendung der übrigen Technologien ist deaktiviert.

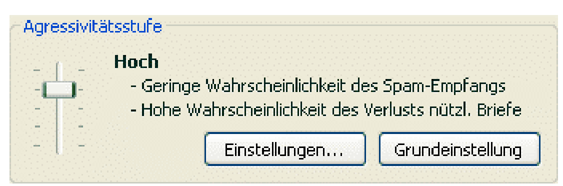


Abbildung 54. Auswahl der Aggressivitätsstufe für Anti-Spam

Hoch – Strenge Stufe, bei deren Verwendung die Wahrscheinlichkeit besteht, dass bestimmte E-Mails, die in Wirklichkeit kein Spam sind, als *Spam* markiert werden. Auf dieser Stufe erfolgt die Analyse eines Briefs mit der weißen und der schwarzen Liste, sowie unter Verwendung der Technologien PDB und GSG und des iBayes-Algorithmus (s. Pkt. 13.3.2 auf S. 202).

Die Verwendung dieses Modus ist dann sinnvoll, wenn sich mit hoher Wahrscheinlichkeit ausschließen lässt, dass die Empfängeradresse den Spam-Absendern unbekannt ist. Beispielsweise, wenn der Empfänger keine E-Mail-Rundschreiben abonniert hat und kein Postfach auf kostenlosen/unternehmensfremden Mailservern besitzt.

Empfohlen – Universelle Stufe (die Klassifikation der E-Mail-Nachrichten betreffend).

Auf dieser Stufe kann es vorkommen, dass unerwünschte Briefe nicht erkannt werden. Dies deutet darauf hin, dass Anti-Spam nicht ausreichend trainiert wurde. Es wird empfohlen, das Modul zusätzlich mit den inkorrekt erkannten Briefen zu trainieren, wozu der Trainingsassistent (s. Pkt. 13.2.1 auf S. 197) oder die Schaltflächen **Spam \ Kein Spam** (für das Programm The Bat! die entsprechenden Menüpunkte) dienen.

Niedrig – Loyalere Stufe. Diese Stufe ist für Benutzer empfehlenswert, deren eingehende Korrespondenz aus einem bestimmten Grund eine große Anzahl von Wörtern enthält, die von Anti-Spam als Spam eingestuft werden, was in diesem Fall aber nicht zutrifft. Der Grund kann in der beruflichen Tätigkeit des Empfängers liegen, bei der im Rahmen der Korrespondenz mit Kollegen professionelle Termini verwendet werden, die häufig in Spam angetroffen werden. Auf dieser Stufe werden zur E-Mail-Analyse alle Technologien zur Spam-Erkennung eingesetzt.

Alle überspringen – Niedrigste Aggressivitätsstufe, auf der nur E-Mails als Spam erkannt werden, die Zeilen aus der schwarzen Wörterliste und Absender, die in der schwarzen Adressenliste genannt sind, enthalten. Auf dieser Stufe erfolgt die Briefanalyse nur mit der schwarzen Liste, die Verwendung der übrigen Technologien ist deaktiviert.

Der Spam-Schutz erfolgt standardmäßig auf der **Empfohlenen** Aggressivitätsstufe.

Sie können die geltende Stufe erhöhen oder senken oder die Einstellungen der gewählten Stufe ändern.

Um die Stufe zu ändern,

verschieben Sie den Zeiger auf der Skala für die Aggressivitätsstufe. Durch das Regulieren der Aggressivitätsstufe bestimmen Sie das Verhältnis der Faktoren für Spam, potentiellen Spam und nützliche Post (s. Pkt. 13.3.3 auf S. 204).

Um die Einstellungen der aktuellen Stufe anzupassen,

klicken Sie im Konfigurationsfenster von Anti-Spam auf die Schaltfläche **Einstellungen**, passen Sie im folgenden Fenster den Spam-Faktor an und klicken Sie auf **OK**.

Dadurch ändert sich die Schutzstufe in **Benutzerdefiniert** und enthält die Schutzparameter, die Sie definiert haben.

13.2. Anti-Spam-Training

Anti-Spam wird mit einer vorinstallierten Nachrichtendatenbank geliefert, die aus fünfzig Spam-Nachrichten besteht. Es wird empfohlen, das Anti-Spam-Modul zusätzlich mit Ihren E-Mail-Nachrichten zu trainieren.

Es existieren mehrere Methoden für das Training von Anti-Spam:

- Verwendung des Trainingsassistenten (Pakettraining) (s. Pkt. 13.2.1 auf S. 197).
- Training von Anti-Spam mit ausgehenden Nachrichten (s. Pkt. 13.2.2 auf S. 198).
- Training direkt während der Arbeit mit der E-Mail-Korrespondenz, wozu die speziellen Schaltflächen in der Symbolleiste des Mailprogramms oder die Menüpunkte dienen (s. Pkt. 13.2.3 auf S. 199).
- Training bei der Arbeit mit den Berichten von Anti-Spam (s. Pkt. 13.2.4 auf S. 200).

Das Training mit Hilfe des Trainingsassistenten sollte möglichst zu Beginn der Arbeit mit Anti-Spam erfolgen. Der Assistent erlaubt es, Anti-Spam mit einer großen Anzahl von E-Mails zu trainieren.

> Beachten Sie, dass das Training mit maximal 50 Briefen aus einem Ordner erfolgt. Wenn ein Ordner mehr Nachrichten enthält, erfolgt das Training nur mit fünfzig E-Mails.

Das zusätzliche Training mit Hilfe der speziellen Schaltflächen an der Oberfläche des Mailprogramms sollte während der Arbeit mit der E-Mail-Korrespondenz verwendet werden.

13.2.1. Trainingsassistent

Der Trainingsassistent erlaubt es, das Anti-Spam-Training im Paketmodus vorzunehmen. Dabei werden die Ordner der Mailbox angegeben, in denen sich Spam und nützliche Post befinden.

Um den Trainingsassistenten zu starten,

1. Wählen Sie im Konfigurationsfenster **Anti-Spam**.

2. Klicken Sie auf der rechten Seite des Konfigurationsfensters auf die Schaltfläche **Trainingsassistent**.

Der Trainingsassistent bietet ein schrittweises Vorgehen zum Training von Anti-Spam. Der Wechsel zum folgenden Schritt des Trainings erfolgt durch Klick auf **Weiter**, die Rückkehr zum vorhergehenden Schritt durch **Zurück**.

Der erste Schritt des Trainingsassistenten besteht in der Auswahl der Ordner, die nützliche Post enthalten. Auf dieser Etappe dürfen nur Ordner gewählt werden, über deren Inhalt vollständige Sicherheit besteht.

Beim zweiten Schritt des Trainingsassistenten werden die Ordner ausgewählt, die Spam enthalten.

Beim dritten Schritt wird mit den von Ihnen gewählten Ordnern das automatische Training von Anti-Spam ausgeführt. Die Anti-Spam-Datenbank wird durch die E-Mail-Nachrichten dieser Ordner ergänzt. Die Absender nützlicher E-Mails werden automatisch in die weiße Adressenliste aufgenommen.

Beim vierten Schritt werden die Trainingsergebnisse auf eine der folgenden Arten gespeichert: Die Trainingsergebnisse werden zur vorhandenen Datenbank hinzugefügt oder die bestehende Datenbank wird durch die Datenbank ersetzt, die beim Training erstellt wurde. Bitte beachten Sie, dass zur korrekten Spam-Erkennung das Training mit mindestens 50 nützlichen und 50 unerwünschten Nachrichten vorgenommen werden muss. Andernfalls funktioniert der iBayes-Algorithmus nicht.

Aus praktischen Gründen beschränkt der Assistent das Training auf 50 Nachrichten in einem ausgewählten Ordner.

13.2.2. Training mit ausgehenden Briefen

Sie können festlegen, dass Anti-Spam mit den ausgehenden Briefen Ihres Mail-Clients trainiert. In diesem Fall wird auf der Grundlage der Analyse von ausgehenden Nachrichten die weiße Adressenliste von Anti-Spam ergänzt. Zum Training werden nur die ersten fünfzig ausgehenden Nachrichten verwendet, danach wird das Training beendet.

Um das Anti-Spam-Training mit ausgehenden Nachrichten zu aktivieren:

1. Wählen Sie im Konfigurationsfenster die Komponenten **Anti-Spam**.

2. Aktivieren Sie das Kontrollkästchen ☑ **Mit ausgehenden E-Mails trainieren** im Abschnitt **Training**.

Achtung!

Das Anti-Spam-Training mit ausgehenden Nachrichten, die mit dem Protokoll MAPI gesendet werden, findet nur statt, wenn das Kontrollkästchen ☑ **Bei Empfang untersuchen** im Erweiterungsmodul von Mail-Anti-Virus für Microsoft Office Outlook aktiviert ist (s. Pkt. 13.3.9 auf S. 213).

13.2.3. Training unter Verwendung Ihres Mailprogramms

Das Training während der unmittelbaren Arbeit mit der E-Mail-Korrespondenz erfolgt unter Verwendung der speziellen Schaltflächen in der Symbolleiste Ihres Mailprogramms.

Bei der Installation auf dem Computer wird Anti-Spam in folgende Mailprogramme integriert:

- Microsoft Office Outlook
- Microsoft Outlook Express
- The Bat!

Die Symbolleiste des Mailprogramms Microsoft Office Outlook enthält dann die beiden Schaltflächen **Spam** und **Kein Spam** und besitzt im Menü **Extras** → **Optionen** die Registerkarte **Anti-Spam** mit den Aktionen (s. Pkt. 13.3.9 auf S. 213). In Microsoft Outlook Express wird neben den Schaltflächen **Spam** und **Kein Spam** in der Symbolleiste die Schaltfläche **Einstellungen** hinzugefügt, mit der das Fenster mit den Aktionen für unerwünschte Post geöffnet wird (s. Pkt. 13.3.10 auf S. 217). Im Mailprogramm The Bat! sind diese Schaltflächen nicht vorhanden und zum Training werden die speziellen Punkte **Als Spam markieren** und **Als KEIN Spam markieren** im Menü **Extras** verwendet.

Wenn Sie sicher sind, dass die gewählte Nachricht Spam ist, klicken Sie auf die Schaltfläche **Spam**. Wenn die Nachricht kein Spam ist, klicken Sie auf **Kein Spam**. Danach führt Anti-Spam am gewählten Brief das Training durch. Wenn Sie mehrere Nachrichten markieren, erfolgt das Training mit allen ausgewählten Briefen.

Achtung!

Wenn Sie gleichzeitig mehrere Nachrichten markieren oder sicher sind, dass ein bestimmter Ordner nur Nachrichten einer Gruppe (Spam oder KEIN Spam) enthält, kann zum Training der Komponente die Paketmethode mit Hilfe des Trainingsassistenten benutzt werden (s. Pkt. 13.2.1 auf S. 197).

13.2.4. Training unter Verwendung der Anti-Spam-Berichte

Es besteht die Möglichkeit zum Training von Anti-Spam auf der Basis von Berichten.

Um die Berichte der Komponente anzuzeigen,

1. Wählen Sie **Anti-Spam** im Abschnitt **Schutz** des Programmhauptfensters.
2. Klicken Sie mit der linken Maustaste auf den Block **Statistik**.

Die Berichte der Komponente erlauben Schlussfolgerungen über die Genauigkeit ihrer Einstellungen. Bei Bedarf kann die Arbeit von Anti-Spam korrigiert werden.

Um eine bestimmte Nachricht als Spam oder KEIN Spam zu markieren,

1. Markieren Sie die Nachricht in der Berichtsliste auf der Registerkarte **Ereignisse** und verwenden Sie die Schaltfläche **Aktionen**.
2. Wählen Sie einen der folgenden Punkt (s. Abb. 55):
   - **Als Spam markieren**
   - **Als KEIN Spam markieren**
   - **Zur weißen Liste hinzufügen**
   - **Zur schwarzen Liste hinzufügen**

Anti-Spam führt am gewählten Brief ein erweitertes Training durch.

13.3. Konfiguration von Anti-Spam

Ein obligatorisches Attribut des Spam-Schutzes stellt das detaillierte Anpassen von Anti-Spam dar. Alle Funktionsparameter der Komponente befinden sich im Konfigurationsfenster von Kaspersky Internet Security und erlauben Ihnen:

- die funktionellen Besonderheiten der Komponente Anti-Spam zu bestimmen (s. Pkt. 13.3.1 auf S. 201).
- die Verwendung unterschiedlicher Technologien zur Spam-Filterung zu wählen (s. Pkt. 13.3.2 auf S. 202).
- die Genauigkeit beim Erkennen von Spam und potentiellem Spam zu regulieren (s. Pkt. 13.3.3 auf S. 204).

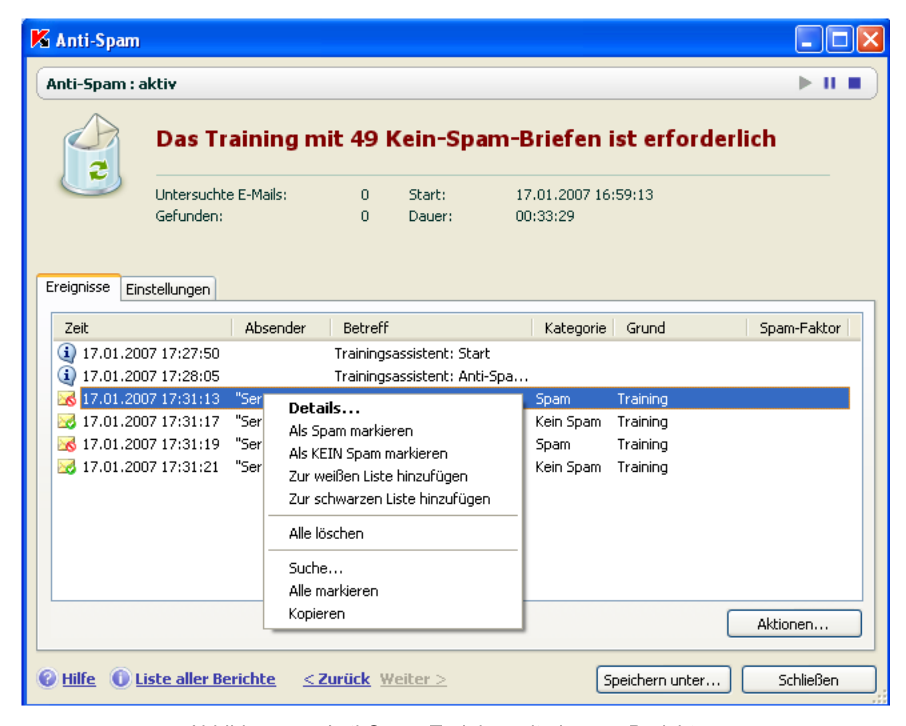


Abbildung 55. Anti-Spam-Training mit eigenen Berichten

- eine schwarze und weiße Liste für Absender und Schlüsselphrasen anzulegen (s. Pkt. 13.3.4 auf S. 205).
- zusätzliche Merkmale der Spam-Filterung anzupassen (s. Pkt. 13.3.5 auf S. 209).
- das Spam-Aufkommen in Ihrer Mailbox aufgrund präventiver Arbeit im Mail-Manager zu minimieren (s. Pkt. 13.3.7 auf S. 211).

In diesem Abschnitt des Handbuchs werden alle oben genannten Parameter ausführlich beschrieben.

13.3.1. Anpassen der Untersuchungseinstellungen

Als Untersuchungsparameter können Sie anpassen:

- Ob der E-Mail-Verkehr der Protokolle POP3 und IMAP untersucht werden soll. Kaspersky Internet Security untersucht standardmäßig die Post aller genannten Protokolle.
- Ob das Erweiterungsmodul (PlugIn) für die Mailprogramme Microsoft Office Outlook und The Bat! aktiviert werden soll.
- Ob jedes Mal, bevor E-Mails mit dem POP3-Protokoll von einem Mailserver in die Mailbox des Benutzers heruntergeladen werden, der Mail-Manager angezeigt werden soll (s. Pkt. 13.3.7 auf S. 211).
-

Um die oben genannten Parameter anzupassen,

1. Wählen Sie die Komponente **Anti-Spam** im Konfigurationsfenster von Kaspersky Internet Security.
2. Aktivieren Sie die entsprechenden Kontrollkästchen im Block **Integration ins System** (s. Abb. 56).
3. Korrigieren Sie bei Bedarf die Netzwerkeinstellungen.



Abbildung 56. Untersuchungsparameter

13.3.2. Auswahl der Technologie zur Spam-Filterung

Die Spam-Analyse von E-Mail-Nachrichten erfolgt unter Verwendung fortschrittlicher Filtertechnologien:

- Die **iBayes-Technologie** basiert auf dem Theorem von Bayes und erlaubt die Analyse des Texts einer E-Mail-Nachricht auf Phrasen, die Spam charakterisieren. Die Analyse beruht auf einer Statistik, die aus dem Anti-Spam-Training hervorgeht (s. Pkt. 13.2 auf S. 197).
- Die **GSG-Technologie** erlaubt die Analyse grafischer Elemente in E-Mail-Nachrichten. Dabei werden zur Identifikation von Spam in Form von Bildern grafische Signaturen verwendet.

- Die **PDB-Technologie** erlaubt die Analyse der Kopfzeilen von E-Mails und die Spam-Klassifikation auf Basis einer Auswahl heuristischer Regeln.

Standardmäßig ist die Verwendung aller Filtertechnologien aktiviert. Dadurch wird gewährleistet, die Spam-Analyse von E-Mail-Nachrichten mit maximaler Sorgfalt vorzunehmen.

Um die Verwendung einer bestimmten Filtertechnologie zu deaktivieren:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security mit dem Link Einstellungen aus dem Programmhauptfenster.

2. Klicken Sie auf die Schaltfläche **Einstellungen** im Block **Aggressivitätsstufe** und gehen Sie im folgenden Fenster auf die Registerkarte **Spam-Erkennung** (s. Abb. 57).

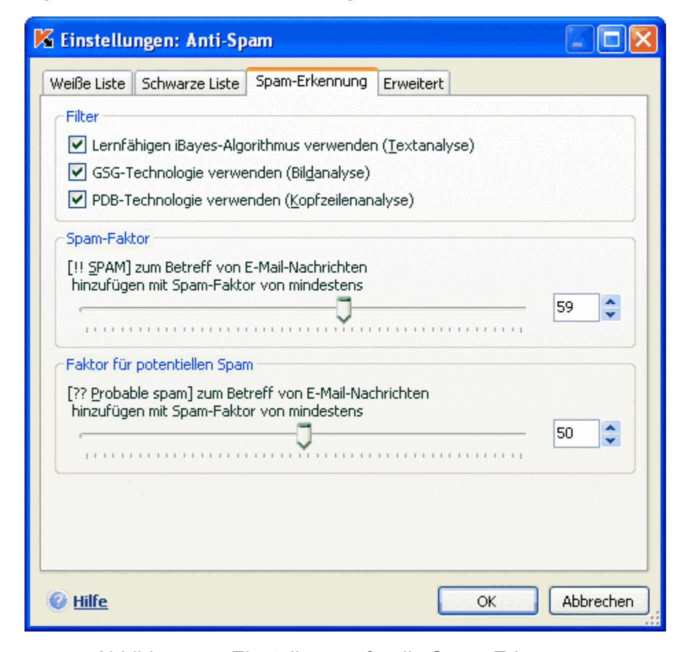


Abbildung 57. Einstellungen für die Spam-Erkennung

3. Deaktivieren Sie die Kontrollkästchen der Filtertechnologien, die Sie bei der Spam-Analyse von E-Mails nicht verwenden möchten.

13.3.3. Definition des Faktors für Spam und potentiellen Spam

Die Kaspersky-Lab-Spezialisten haben sich bemüht, Anti-Spam möglichst umfassend für die Unterscheidung von Spam und potentiellem Spam einzustellen.

Die Spam-Erkennung basiert auf der Verwendung fortschrittlicher Technologien (s. Pkt. 13.3.2 auf S. 202), die es erlauben, Anti-Spam mit einer bestimmten Anzahl von Nachrichten aus Ihrer Mailbox möglichst genau zu trainieren, um zwischen Spam, potentiellem Spam und nützlicher Post zu unterscheiden.

Das Anti-Spam-Training erfolgt bei der Arbeit des Trainingsassistenten und beim Training mit Mailprogrammen. Dabei wird jedem einzelnen Element aus nützlicher Post oder Spam ein bestimmter Koeffizient zugeordnet. Wenn in Ihrer Mailbox eine E-Mail-Nachricht eingeht, untersucht Anti-Spam den Brief mit der iBayes-Technologie auf die Existenz von Elementen aus Spam und nützlicher Post. Die Koeffizienten jedes Elements werden summiert und der *Spam-Faktor* und *potentielle Spam-Faktor* werden errechnet.

Der Faktor für potentiellen Spam bestimmt die Wahrscheinlichkeit, mit der eine Nachricht als potentieller Spam klassifiziert wird. Bei Verwendung der **Empfohlenen** Stufe gilt jede Nachricht mit einer Wahrscheinlichkeit von über 50 % und unter 59 % als *potentieller Spam*. Als nützliche Post gelten Nachrichten, bei deren Untersuchung die Wahrscheinlichkeit unter 50 % liegt.

Der Spam-Faktor bestimmt die Wahrscheinlichkeit, mit der Anti-Spam eine E-Mail-Nachricht als Spam klassifiziert. Jede Nachricht, deren Wahrscheinlichkeit über der angegeben liegt, wird als Spam betrachtet. Für die **Empfohlene** Stufe beträgt der standardmäßige Spam-Faktor 59 %. Das bedeutet, dass jede Nachricht mit einer Wahrscheinlichkeit von über 59 % als Spam markiert wird.

Insgesamt sind fünf Aggressivitätsstufen vorgesehen (s. Pkt. 13.1 auf S. 195), von denen drei (**Hoch**, **Empfohlen** und **Niedrig**) auf unterschiedlichen Werten der Faktoren für Spam und potentiellen Spam basieren.

Auf folgende Weise können Sie den Algorithmus für die Arbeit von Anti-Spam selbständig korrigieren:

1. Wählen Sie im Konfigurationsfenster von Kaspersky Internet Security **Anti-Spam**.
2. Klicken Sie auf der rechten Seite des Fensters im Block **Aggressivitätsstufe** auf die Schaltfläche **Einstellungen**.
3. Regulieren Sie im folgenden Fenster auf der Registerkarte **Spam-Erkennung** (s. Abb. 57) in den entsprechenden Blöcken die Faktoren für Spam und potentiellen Spam.

13.3.4. Erstellen der schwarzen und weißen Liste

Die schwarze und die weiße Liste werden vom Benutzer manuell erstellt und beruhen auf der Arbeit der Komponente Anti-Spam mit den E-Mails. In diese Listen werden Informationen eingetragen, welche sich auf Benutzeradressen beziehen, deren E-Mails eindeutig als nützlich oder aber als Spam gelten, sowie unterschiedliche charakteristische Zeilen und Schlüsselwörter, auf deren Basis sich eine E-Mail als erwünscht oder unerwünscht identifizieren lässt.

Der Hauptvorteil der Schlüsselwortlisten und der weißen Liste besteht darin, dass Sie mit zuverlässigen Adressaten (beispielsweise mit Kollegen) vereinbaren können, Ihre Korrespondenz mit einer bestimmten Zeile zu signieren. Dabei kann es sich um eine beliebige Zeile handeln. Als "Signaturzeile" können Sie beispielsweise einen PGP-Signatur verwenden. Sowohl in Signaturen als auch in Adressen ist die Verwendung der Platzhalterzeichen ***** und **?** zulässig. Das Zeichen ***** steht für eine beliebige Zeichenfolge mit beliebiger Länge. Das Zeichen **?** steht für ein beliebiges einzelnes Zeichen.

Wenn die Zeichen ***** und **?** zu einer Signatur gehören, muss ihnen das neutralisierende Zeichen \ vorangestellt werden, damit Sie von Anti-Spam nicht als Platzhalter interpretiert werden. In diesem Fall werden anstelle eines Zeichens zwei verwendet: ***** und **\?**.

13.3.4.1. Weiße Adressen- und Zeilenliste

In der weißen Liste werden Schlüsselphrasen der Nachrichten gespeichert, die Sie als *KEIN Spam* markiert haben, und die Adressen der Absender, von denen Ihrer Meinung nach kein Spam eintreffen sollte. Die weiße Zeilenliste wird manuell ergänzt, die Liste der Absenderadressen wird während dem Training der Komponente Anti-Spam automatisch erstellt.

Um zur Konfiguration der weißen Liste zu wechseln,

1. Wählen Sie **Anti-Spam** im Konfigurationsfenster von Kaspersky Internet Security.
2. Klicken Sie auf der rechten Seite des Konfigurationsfensters auf die Schaltfläche **Einstellungen**.
3. Öffnen Sie die Registerkarte **Weiße Liste** (s. Abb. 58).

Die Registerkarte besteht aus zwei Blöcken: Im oberen Block stehen die Absenderadressen nützlicher Post, im unteren Block die Schlüsselphrasen solcher Nachrichten.

Um die Verwendung der weißen Listen für Wörter und Adressen bei der Spam-Filterung zu aktivieren, setzen Sie die entsprechenden Kontrollkästchen in den Blöcken **Zulässige Absender** und **Zulässige Wörter**.

Jeder Block verfügt über Schaltflächen zum Bearbeiten der Listen.

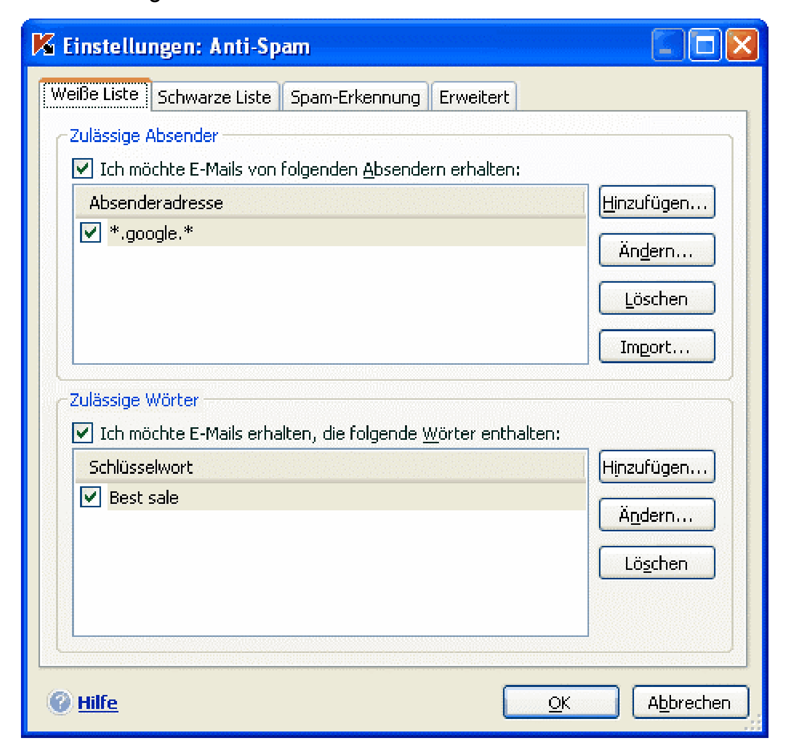


Abbildung 58. Anpassen der weißen Listen für Adressen und Wörter

Als Adresse einer Liste können sowohl Adressen als auch Adressenmasken benutzt werden. Groß- und Kleinschreibung werden bei der Adressenangabe ignoriert. Im Folgenden werden Beispiele für Adressenmasken genannt:

- *hammer@test.de* – E-Mail-Nachrichten von dem Absender mit dieser Adresse werden immer als nützliche Post klassifiziert.
- **@test.de* – Post von einem beliebigen Absender der Maildomäne *test.de* gilt als nützlich. Beispiele: *hinze@test.de*, *kunze@test.de*;
- *hammer@** – Ein Absender mit diesem Namen sendet unabhängig von der Maildomäne nur nützliche Post. Beispiele: *hammer@test.de*, *hammer@mail.de*;

- **@test** – Post eines beliebigen Absenders einer Maildomäne, die mit *test* beginnt, ist kein Spam. Beispiele: *hammer@test.de*, *hinze@test.com*;
- *hans.*@test.???* – Post von einem Absender, dessen Name mit *hans.* beginnt und dessen Maildomäne mit *test* beginnt und mit drei beliebigen Zeichen endet, gilt immer als nützlich. Beispiele: *hans.hammer@test.com*, *hans.hinze@test.org*.

Auch als Zeilen können Masken verwendet werden. Groß- und Kleinschreibung werden bei der Maskenangabe ignoriert. Es folgen einige Beispiele:

- *Hallo Hans!* – Eine Nachricht, die nur diesen Text enthält, gilt als nützlich. Es wird nicht geraten, derartige Zeilen als Zeilen der weißen Liste zu verwenden.
- *Hallo Hans!** – Eine Nachricht, die mit der Zeile *Hallo Hans!* beginnt, gilt als nützlich.
- *Hallo *! ** – Eine Nachricht, die mit dem Grußwort *Hallo* beginnt und an einer beliebigen Stelle ein Ausrufezeichen enthält, gilt nicht als Spam.
- ** Hans? ** – Eine Nachricht, welche die Begrüßung eines Benutzers mit dem Namen *Hans* enthält, nach dessen Namen ein beliebiges Zeichen folgt, ist kein Spam.
- ** Hans\? ** – Eine Nachricht, welche die Zeile *Hans?* enthält, gilt als nützlich.

Wenn Sie eine bestimmte Adresse oder Phrase vorübergehend nicht als Attribut nützlicher Post verwenden möchten, muss diese nicht unbedingt aus der Liste gelöscht werden. Es ist ausreichend, die entsprechenden Kontrollkästchen zu deaktivieren.

Für die Adressen der weißen Liste ist eine Option zum Import aus einer Datei des Formats CSV (Comma Separated Values – durch Komma getrennte Werte) vorgesehen.

13.3.4.2. Schwarze Adressen- und Zeilenliste

In der schwarzen Absenderliste werden Schlüsselphrasen der Nachrichten gespeichert, die Ihrer Meinung nach *Spam* sind, und die Adressen ihrer Absender. Die Liste wird manuell ergänzt.

Um zur Konfiguration der schwarzen Liste zu wechseln,

1. Wählen Sie **Anti-Spam** im Konfigurationsfenster von Kaspersky Internet Security.
2. Klicken Sie auf der rechten Seite des Konfigurationsfensters auf die Schaltfläche **Einstellungen**.

3. Öffnen Sie die Registerkarte **Schwarze Liste** (s. Abb. 59).

Die Registerkarte besteht aus zwei Blöcken: Im oberen Block stehen die Adressen von Spam-Absendern, im unteren Block die Schlüsselphrasen solcher Nachrichten.

Um die Verwendung der schwarzen Listen für Wörter und Adressen bei der Spam-Filterung zu aktivieren, setzen Sie die entsprechenden Kontrollkästchen in den Blöcken **Verbotene Absender** und **Verbotene Wörter**.

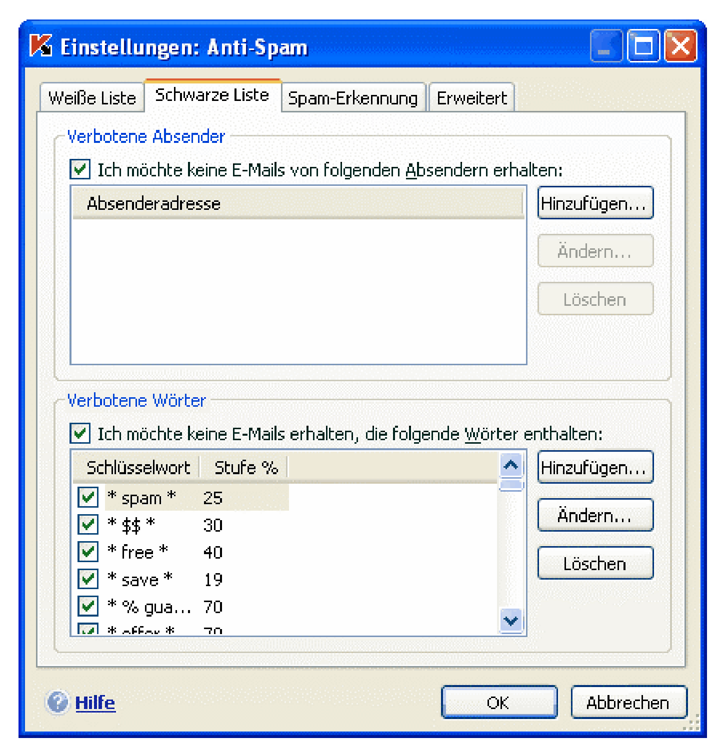


Abbildung 59. Anpassen der schwarzen Listen für Adressen und Wörter

Jeder Block verfügt über Schaltflächen zum Bearbeiten der Listen.

Als Adresse einer Liste können sowohl Adressen als auch Adressenmasken benutzt werden. Groß- und Kleinschreibung werden bei der Adressenangabe ignoriert. Im Folgenden werden Beispiele für Adressenmasken genannt:

- *hammer@test.de* – E-Mail-Nachrichten von dem Absender mit dieser Adresse werden immer als Spam klassifiziert.

- **@test.de* – Post von einem beliebigen Absender der Maildomäne *test.de* gilt als Spam. Beispiele: *hinze@test.de*, *kunze@test.de*;
- *hammer@** – Ein Absender mit diesem Namen sendet unabhängig von der Maildomäne nur Spam. Beispiele: *hammer@test.de*, *hammer@mail.de*;
- **@test** – Post eines beliebigen Absenders einer Maildomäne, die mit *test* beginnt, ist Spam. Beispiele: *hammer@test.de*, *hinze@test.com*;
- *hans.*@test.???* – Post von einem Absender, dessen Name mit *hans.* beginnt und dessen Maildomäne mit *test* beginnt und mit drei beliebigen Zeichen endet, gilt immer als Spam. Beispiele: *hans.hammer@test.com*, *hans.hinze@test.org*.

Auch als Zeilen können Masken verwendet werden. Groß- und Kleinschreibung werden bei der Maskenangabe ignoriert. Es folgen einige Beispiele:

- *Hallo Hans!* – Eine Nachricht, die nur diesen Text enthält, gilt als Spam. Es wird nicht geraten, derartige Zeilen als Zeilen der Liste zu verwenden.
- *Hallo Hans!** – Eine Nachricht, die mit der Zeile *Hallo Hans!* beginnt, gilt als Spam.
- *Hallo *! ** – Eine Nachricht, die mit dem Grußwort *Hallo* beginnt und an einer beliebigen Stelle ein Ausrufezeichen enthält, gilt als Spam.
- ** Hans? ** – Eine Nachricht, welche die Begrüßung eines Benutzers mit dem Namen *Hans* enthält, nach dessen Namen ein beliebiges Zeichen folgt, ist Spam.
- ** Hans\? ** – Eine Nachricht, welche die Zeile *Hans?* enthält, gilt als Spam.

Wenn Sie eine bestimmte Adresse oder Phrase vorübergehend nicht als obligatorische Spam-Merkmale verwenden möchten, müssen diese nicht unbedingt aus der Liste gelöscht werden. Es ist ausreichend, die entsprechenden Kontrollkästchen zu deaktivieren.

13.3.5. Zusatzmerkmale bei der Spam-Filterung

Neben den Hauptmerkmalen, auf deren Grundlage die Spam-Filterung von Nachrichten erfolgt (Erstellen der weißen und schwarzen Listen, Phishing-Analyse, Analyse mit Hilfe der Filtertechnologien) können Sie zusätzliche Merkmale festlegen.

Zur Konfiguration der Zusatzmerkmale für die Spam-Filterung von E-Mails:

1. Wählen Sie im Konfigurationsfenster von Kaspersky Internet Security die Komponente **Anti-Spam.**
2. Klicken Sie auf die Schaltfläche **Einstellungen** auf der rechten Seite des Konfigurationsfensters.
3. Öffnen Sie die Registerkarte **Erweitert** (s. Abb. 60).

Diese Liste bietet eine Liste der Merkmale, auf deren Grundlage einer Nachricht der Status *Spam* mit einer bestimmten Wahrscheinlichkeitsstufe zugewiesen wird.

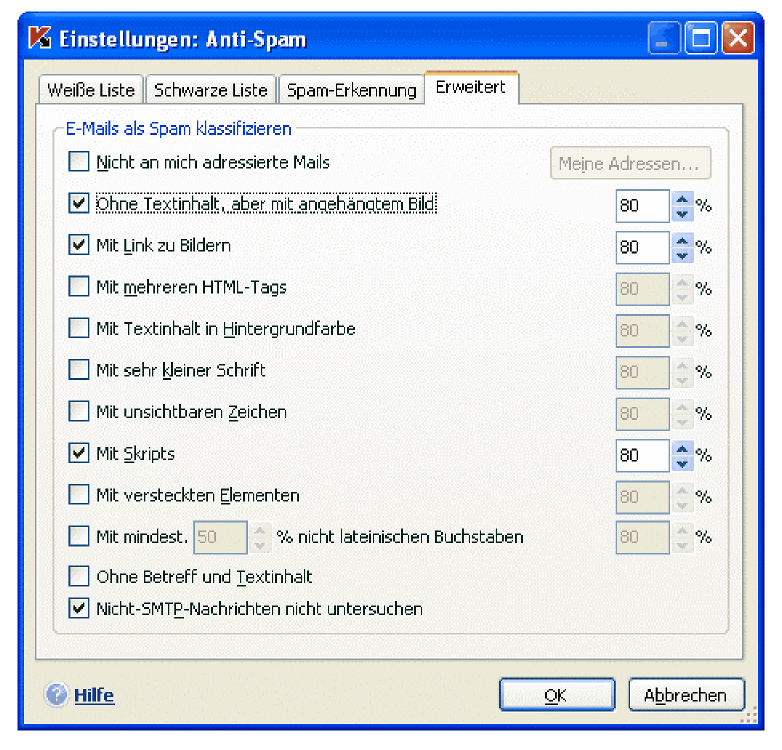


Abbildung 60. Erweiterte Einstellungen für die Spam-Erkennung

Um die Verwendung eines bestimmten zusätzlichen Filtermerkmals zu aktivieren, aktivieren Sie das entsprechende Kontrollkästchen. Außerdem muss für jedes ausgewählte Merkmal ein Spam-Faktor (in Prozent) festgelegt werden, der die Wahrscheinlichkeit bestimmt, mit welcher ein Brief als Spam klassifiziert wird. Der Spam-Faktor beträgt standardmäßig 80 %. Eine Nachricht wird als

Spam markiert, wenn die Summe der Wahrscheinlichkeiten für alle Zusatzmerkmale über 100 % liegt.

Wenn Sie die Filterung nach dem Merkmal "Nicht an mich adressiert" wählen, muss eine Liste Ihrer Adressen angelegt werden. Dazu dient das Fenster, das mit der Schaltfläche **Meine Adressen** geöffnet wird.

13.3.6. Erstellen einer Liste mit vertrauenswürdigen Adressen

Wenn Sie die Spam-Filterung für E-Mails nach dem Merkmal "Nicht an mich adressiert" aktiviert haben, ist die Angabe Ihrer vertrauenswürdigen E-Mail-Adressen erforderlich.

Bei der Spam-Analyse wird die Empfängeradresse überprüft. Wenn die Adresse nicht mit einer Adresse Ihrer Liste übereinstimmt, erhält der Brief den Status *Spam*.

Zum Erstellen und Ändern der Adressenliste dienen die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** im Fenster **Meine E-Mail-Adressen**.

13.3.7. Mail-Manager

Achtung!

Der Mail-Manager steht nur zur Verfügung, wenn Sie die Post mit dem Protokoll POP3 empfangen.

Der Mail-Manager dient zur Ansicht einer Liste der auf dem Server vorhandenen E-Mail-Nachrichten, ohne sie auf Ihren Computer herunterzuladen. Das erlaubt, den Empfang bestimmter Nachrichten abzulehnen, wodurch nicht nur Zeit und Geld bei der Arbeit mit elektronischer Post eingespart werden können, sondern auch die Wahrscheinlichkeit des Downloads von Spam und Viren auf Ihren Computer verringert wird.

Der Mail-Manager wird geöffnet, wenn in den Einstellungen von Anti-Spam das Kontrollkästchen ☑ **Mail-Manager bei Mailempfang öffnen** aktiviert wurde.

Um Nachrichten auf dem Server zu löschen, ohne sie auf Ihren Computer herunterzuladen,

> aktivieren Sie die Kontrollkästchen rechts der Briefe, die gelöscht werden sollen, und klicken Sie auf die Schaltfläche **Löschen**. Die zu löschenden Nachrichten werden vom Server gelöscht. Die übrige Korrespondenz wird

nach dem Schließen des Mail-Manager-Fensters auf Ihren Computer heruntergeladen.

Wenn man nur die Daten über den Absender und die Betreffzeile der Nachricht kennt, ist es manchmal schwierig zu entscheiden, ob eine E-Mail-Nachricht empfangen werden soll. In solchen Fällen bietet der Mail-Manager Ihnen erweiterte Informationen über den Brief, wozu die Kopfzeilen heruntergeladen werden.

Um die Kopfzeilen einer Nachricht zu lesen,

markieren Sie die Nachricht in der Liste der eingehenden Korrespondenz. Die Kopfzeilen der Nachricht werden im unteren Bereich des Formulars angezeigt.

Die Kopfzeilen von Nachrichten besitzen eine geringe Größe, die nur wenige Bit beträgt, und können keinen schädlichen Code enthalten.

Das Lesen von Kopfzeilen kann beispielsweise in folgender Situation nützlich sein: Spammer haben auf dem Computer Ihres Kollegen ein Schadprogramm installiert, das unter seinem Namen Spam verschickt und dabei das Adressbuch seines Mailprogramms verwendet. Die Wahrscheinlichkeit, dass Sie sich im Adressbuch Ihres Kollegen befinden, ist sehr hoch, was zweifellos dazu führt, dass Ihre Mailbox mit Spam von Ihrem Kollegen überfüllt wird. In dieser Situation ist es unmöglich, allein aufgrund der Absenderadresse zu ermitteln, ob eine Nachricht von Ihrem Kollegen oder dem Spammer abgeschickt wurde. Verwenden Sie die Kopfzeilen der Nachricht! Überprüfen Sie sorgfältig, von wem und wann der Brief abgesandt wurde und wie groß er ist. Verfolgen Sie den Weg der Nachricht vom Absender auf Ihren Mailserver. Alle entsprechenden Informationen befinden sich in den Kopfzeilen der Nachricht. Entscheiden Sie, ob diese E-Mail wirklich vom Server heruntergeladen oder besser gelöscht werden soll.

Hinweis:

Die Nachrichten können nach einer beliebigen Spalte der Nachrichtenliste sortiert werden. Klicken Sie zum Sortieren auf die Spaltenüberschrift. Die Zeilen werden aufsteigend sortiert. Um die Sortierrichtung zu wechseln, klicken Sie erneut auf die Spaltenüberschrift.

13.3.8. Aktionen für unerwünschte Post

Wenn sich aufgrund einer Untersuchung ergibt, dass eine Nachricht als Spam oder potentieller Spam gilt, sind die weiteren Operationen von Anti-Spam vom Status des Objekts und der ausgewählten Aktion abhängig. Standardmäßig werden E-Mail-Nachrichten, die als *Spam* oder *potentieller Spam* gelten,

modifiziert: Im Feld **Betreff** der Nachricht wird die Markierung **[!! SPAM]** bzw. **[?? Probable Spam]** hinzugefügt.

Sie können Zusatzaktionen für Spam und potentiellen Spam festlegen. In den Mailprogrammen Microsoft Office Outlook, Microsoft Outlook Express und The Bat! sind dafür spezielle Erweiterungsmodule vorgesehen. Für andere Mailprogramme können Sie Filterregeln erstellen.

13.3.9. Anpassen der Spam-Bearbeitung in Microsoft Office Outlook

Beachten Sie, dass das PlugIn zu Spam-Untersuchung von E-Mails für Microsoft Office Outlook nicht zur Verfügung steht, wenn die Anwendung auf einem Computer mit Microsoft Windows 9x installiert ist.

Diese Option wird auf Computern mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition und Microsoft Windows Vista x64 nur für die 32-Bit-Version des Mailprogramms Microsoft Office Outlook unterstützt.

E-Mails, die Anti-Spam als *Spam* oder *potentiellen Spam* klassifiziert, wird standardmäßig durch die speziellen Markierungen **[!! SPAM]** bzw. **[?? Probable Spam]** im Feld **Betreff** gekennzeichnet.

Zusätzliche Aktionen für Spam und potentiellen Spam werden in Microsoft Office Outlook auf der speziellen Registerkarte **Anti-Spam** im Menü **Extras** → **Optionen** angepasst (s. Abb. 61).

Diese Registerkarte wird beim ersten Start des Mailprogramms nach der Installation des Programms automatisch geöffnet, und Ihnen wird angeboten, die Bearbeitung von unerwünschter Post zu konfigurieren.

Sowohl für Spam als auch für potentiellen Spam können Sie folgende Bearbeitungsregeln festlegen:

Verschieben in Ordner – Unerwünschte Post wird in den von Ihnen gewählten Mailbox-Ordner verschoben.

Kopieren in Ordner – Eine Kopie der Nachricht wird angelegt und in den gewählten Ordner verschoben. Die Originalnachricht verbleibt im Ordner **Posteingang**.

Löschen – Unerwünschte Post wird aus der Mailbox des Benutzers gelöscht.

Überspringen – Die Nachricht verbleibt im Ordner **Posteingang**.



Abbildung 61. Detaillierte Konfiguration der Spam-Bearbeitung in Microsoft Office Outlook

Wählen Sie dazu im Block **Spam** oder **Potentieller Spam** den entsprechenden Wert aus der Dropdown-Liste.

Außerdem können Sie den Algorithmus für die Zusammenarbeit von Microsoft Office Outlook und des PlugIns von Anti-Spam festlegen:

- **Bei Empfang untersuchen**. Alle Nachrichten, die in der Mailbox des Benutzers eintreffen, werden zuerst in Übereinstimmung mit den für Microsoft
Office Outlook festgelegten Regeln bearbeitet. Nach Abschluss dieser Bearbeitung werden die übrigen Nachrichten, die unter keine Regel fallen, zur Bearbeitung an das Erweiterungsmodul von Anti-Spam übergeben. Die Bearbeitung der Nachrichten erfolgt also in einer bestimmten Reihenfolge. Es kann vorkommen, dass diese Reihenfolge unterbrochen wird. Dies kann beispielsweise der Fall sein, wenn gleichzeitig sehr viele Briefe in der

Mailbox eintreffen. Dadurch können Informationen über einen Brief, der nach einer Microsoft Office Outlook-Regel bearbeitet wurde, mit dem Status *Spam* im Bericht von Anti-Spam eingetragen werden. Um dies zu vermeiden, empfehlen wir, die Arbeit des Anti-Spam-PlugIns als Microsoft Office Outlook-Regel zu konfigurieren.

- **Verwenden einer Microsoft Outlook-Regel**. In diesem Fall werden die Nachrichten, die in der Benutzermailbox eintreffen, entsprechend der Hierarchie der für Microsoft Office Outlook erstellten Regeln bearbeitet. Dabei muss eine Regel für die Nachrichtenbearbeitung durch Anti-Spam erstellt werden. Dieser Algorithmus gilt für die Arbeit als optimal, da keine Konflikte zwischen Microsoft Office Outlook und dem Anti-Spam-Erweiterungsmodul auftreten. Die einzige Unzulänglichkeit dieses Algorithmus besteht darin, dass die Regel zur Spam-Bearbeitung von Nachrichten manuell über Microsoft Office Outlook erstellt bzw. gelöscht werden muss.

> Die Verwendung des Anti-Spam-Erweiterungsmoduls als Regel für Microsoft Office Outlook wird in der Version Microsoft Office Outlook XP nicht unterstützt, wenn sie unter dem Betriebssystem Microsoft Windows 9x/ME/NT4 installiert ist. Dies geht auf einen Fehler im Programm Microsoft Office Outlook XP zurück.

Um eine Regel zur Spam-Bearbeitung von Nachrichten zu erstellen:

1. Starten Sie das Programm Microsoft Office Outlook und verwenden Sie den Befehl **Extras→Regeln und Benachrichtigungen** im Programmhauptfenster. Der Befehl zum Aufrufen des Assistenten ist von Ihrer Microsoft Office Outlook-Version abhängig. In diesem Handbuch wird das Erstellen einer Regel mit Hilfe von Microsoft Office Outlook 2003 beschrieben.

2. Gehen Sie im Fenster **Regeln und Benachrichtigungen** auf die Registerkarte **Regeln für E-Mails** und klicken Sie auf die Schaltfläche **Neu**. Dadurch wird der Assistent zum Erstellen einer neuen Regel gestartet. Seine Arbeit besteht aus einer Folge von Fenstern/Schritten:

   Schritt 1.

   Sie können wählen, ob zum Erstellen der Regel eine Vorlage benutzt werden soll oder nicht. Wählen Sie die Variante **Regel ohne Vorlage erstellen** und wählen Sie als Prüfungsbedingung **Nachrichten bei Ankunft prüfen**. Klicken Sie auf die Schaltfläche **Weiter**.

   Schritt 2.

   Klicken Sie im Fenster zur Auswahl der Bedingungen für die Nachrichtenprüfung auf die Schaltfläche **Weiter**, ohne ein Kontrollkästchen zu aktivieren. Bestätigen Sie die Anwendung dieser Regel auf alle Nachrichten, die Sie erhalten.

Schritt 3.

Aktivieren Sie im Fenster zur Auswahl der Aktionen für die Nachrichten in der Aktionsliste das Kontrollkästchen ☑ **diese mit einer vordefinierten Aktion bearbeiten**. Klicken Sie im unteren Bereich des Fensters auf den Link einer vordefinierten Aktion. Wählen Sie aus der Dropdown-Liste den Wert **Kaspersky Anti-Spam** und klicken Sie auf **OK**.

Schritt 4.

Klicken Sie im Fenster zur Auswahl von Ausnahmen auf die Schaltfläche **Weiter**, ohne ein Kontrollkästchen zu aktivieren.

Schritt 5.

Im Fenster zum Abschluss der Regelerstellung können Sie den Namen der Regel ändern (standardmäßig lautet er **Kaspersky Anti-Spam**). Überprüfen Sie, ob das Kontrollkästchen ☑ **Diese Regel aktivieren** aktiviert ist und klicken Sie auf die Schaltfläche **Fertig stellen**.

3. Die neue Regel wird standardmäßig an erste Stelle zur Regelliste im Fenster **Regeln und Benachrichtigungen** hinzugefügt. Wenn Sie möchten, dass die Regel zuletzt auf eine Nachricht angewandt wird, verschieben Sie sie an das Ende der Liste.

Alle Nachrichten, die in der Mailbox ankommen, werden auf der Grundlage von Regeln bearbeitet. Die Verwendungsreihenfolge der Regeln hängt von der Priorität der einzelnen Regeln ab. Die Regeln werden nacheinander verwendet, wobei mit der obersten Regel begonnen wird. Die oberste Regel der Liste besitzt die höchste Priorität, jede folgende Regel eine niedrige. Sie können die Anwendungspriorität der Regeln erhöhen oder senken.

Wenn Sie nicht möchten, dass eine Nachricht zusätzlich nach einer Anti-Spam-Regel bearbeitet wird, nachdem bereits eine Regel angewandt wurde, muss in den Einstellungen dieser Regel das Kontrollkästchen ☑ **keine weiteren Regeln anwenden** aktiviert werden (s. Schritt 3. zum Erstellen der Regel).

Wenn Sie über Erfahrung beim Erstellen von Bearbeitungsregeln für E-Mail-Nachrichten in Microsoft Office Outlook verfügen, können Sie auf der Basis des oben vorgeschlagenen Algorithmus eine eigene Regel für Anti-Spam erstellen.

13.3.10. Anpassen der Spam-Bearbeitung in Microsoft Outlook Express

E-Mail-Korrespondenz, die Anti-Spam als *Spam* oder *potentieller Spam* klassifiziert, wird standardmäßig durch die speziellen Markierungen **[!! SPAM]** bzw. **[?? Probable Spam]** im Feld **Betreff** gekennzeichnet.

Zusätzliche Aktionen für Spam und potentiellen Spam werden in Microsoft Office Outlook Express in dem speziellen Fenster angepasst (s. Abb. 62), das durch die Schaltfläche **Einstellungen** geöffnet wird, die sich neben den anderen Anti-Spam-Schaltflächen **Spam** und **Kein Spam** in der Symbolleiste befinden.



Abbildung 62. Detaillierte Konfiguration der Spam-Bearbeitung in Microsoft Outlook Express

Das Fenster wird beim ersten Start des Mailprogramms nach der Installation des Programms automatisch geöffnet, und Ihnen wird angeboten, die Bearbeitung von unerwünschter Post zu konfigurieren.

Sowohl für Spam als auch für potentiellen Spam können Sie folgende Bearbeitungsregeln festlegen:

Verschieben in Ordner – Unerwünschte Post wird in den von Ihnen gewählten Mailbox-Ordner verschoben.

Kopieren in Ordner – Eine Kopie der Nachricht wird angelegt und in den gewählten Ordner verschoben. Die Originalnachricht verbleibt im Ordner **Posteingang**.

Löschen – Unerwünschte Post wird aus der Mailbox des Benutzers gelöscht.

Überspringen – Die Nachricht verbleibt im Ordner **Posteingang**.

Wählen Sie dazu im Block **Spam** oder **Potentieller Spam** den entsprechenden Wert aus der Dropdown-Liste.

13.3.11. Anpassen der Spam-Bearbeitung in The Bat!

Diese Option wird auf Computern mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition und Microsoft Windows Vista x64 nur für die 32-Bit-Version des Mailprogramms The Bat! unterstützt.

Die Aktionen für Spam und potentiellen Spam werden im Mailprogramm The Bat! mit den Mitteln des Mailprogramms festgelegt.

Um in The Bat! zur Konfiguration der Bearbeitungsregeln für Spam zu wechseln,

1. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Anti-Spam-Plugins** (s. Abb. 63).

Die angezeigten Parameter für den Spam-Schutz gelten für alle auf dem Computer installierten Anti-Spam-Module, welche die Arbeit mit The Bat! unterstützen.

Sie müssen eine Score-Stufe festlegen und angeben, wie mit Nachrichten eines bestimmten Scores (im Fall von Anti-Spam ist das die Wahrscheinlichkeit, dass ein Brief als Spam gilt) verfahren werden soll:

- Nachricht mit einem Score über der angegebenen Größe löschen.
- Nachricht mit einem bestimmten Score in einen speziellen Ordner für Spam-Nachrichten verschieben.

- Spam-Nachrichten, die mit einer speziellen Kopfzeile markiert sind, in den Spam-Ordner verschieben.
- Spam-Nachrichten im Ordner **Eingang** belassen.

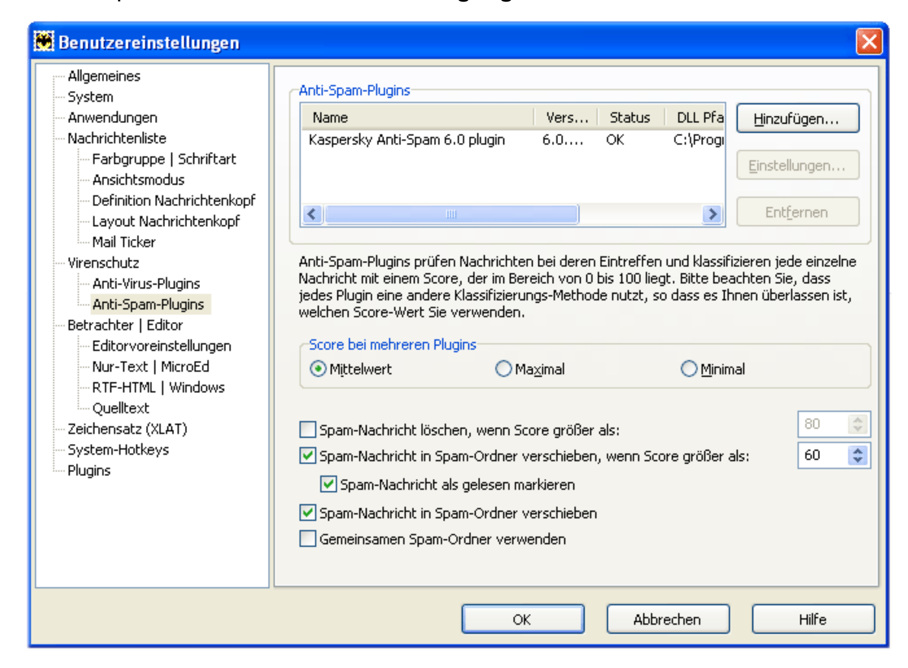


Abbildung 63. Konfiguration der Spam-Erkennung und –Bearbeitung in The Bat!

> Achtung!
>
> Aufgrund der Bearbeitung von E-Mail-Nachrichten durch Kaspersky Internet Security wird der Nachricht auf der Basis eines Faktors (s. Pkt. 13.3.3 auf S. 204), den Sie festlegen können, der Status *Spam* oder *potentieller Spam* zugewiesen. Im Mailprogramm The Bat! ist ein entsprechender Score-Algorithmus für Nachrichten realisiert, der den Gegenstand Spam betrifft, und ebenfalls auf dem Spam-Faktor basiert. Damit die Spam-Faktoren in Kaspersky Internet Security und in The Bat! nicht differieren, werden alle von Anti-Spam überprüften Nachrichten dem Rating angepasst, das dem Status der Nachricht entspricht: *nützliche Post* – 0%, *potentieller Spam – 50 %*, *Spam – 100 %*.
>
> Dadurch stimmt der Score der Nachricht im Mailprogramm The Bat! nicht mit dem in Anti-Spam festgelegten Faktor der Nachricht überein, sondern mit dem Faktor des entsprechenden Status.

Einzelheiten über den Spam-Score und die Bearbeitungsregeln s. Dokumentation zum Mailprogramm The Bat!

KAPITEL 14. VIRENSUCHE AUF IHREM COMPUTER

Ein wichtiger Bestandteil des Antivirenschutzes für einen Computer ist die Virensuche in vom Benutzer festgelegten Bereichen. Kaspersky Internet Security 6.0 erlaubt es, sowohl einzelne Objekte (Dateien, Ordner, Laufwerke, Wechseldatenträger) als auch den gesamten Computer auf das Vorhandensein von Viren zu untersuchen. Durch die Virensuche lässt sich die Möglichkeit der Ausbreitung eines schädlichen Codes verhindern, der von den Schutzkomponenten aus bestimmten Gründen nicht erkannt wurde.

Kaspersky Internet Security 6.0 verfügt über drei standardmäßige Untersuchungsaufgaben:

Kritische Bereiche

Virenuntersuchung aller kritischen Computerbereiche sowie Virenuntersuchung aller Objekte, die am Systemstart beteiligt sind. Dazu gehören: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Laufwerksbootsektoren und *Windows*-Systemverzeichnisse. Das Ziel dieser Aufgabe besteht im schnellen Auffinden von im System aktiven Viren, ohne dazu die vollständige Untersuchung des Computers zu starten.

Arbeitsplatz

Virensuche auf Ihrem Computer mit sorgfältiger Untersuchung aller angeschlossenen Laufwerke, des Arbeitsspeichers und der Dateien.

Autostart-Objekte

Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

Diese Aufgaben werden standardmäßig mit den empfohlenen Einstellungen ausgeführt. Sie können diese Einstellungen ändern (s. Pkt. 14.4 auf S. 226) und einen Zeitplan für den Aufgabenstart festlegen (s. Pkt. 6.5 auf S. 91).

Außerdem besteht die Möglichkeit, eigene Aufgaben zur Virensuche zu erstellen (s. Pkt. 14.3 auf S. 224) und einen Startzeitplan dafür anzulegen. Es kann beispielsweise eine Aufgabe zur wöchentlichen Untersuchung von Maildatenbanken oder eine Aufgabe zur Virensuche im Ordner **Eigene Dateien** erstellt werden.

Daneben können Sie ein beliebiges Objekt auf Viren untersuchen (z.B. eine Festplatte, auf der sich Programme und Spiele befinden, Maildatenbanken, die

aus dem Büro mitgebracht wurden, ein Archiv, das per E-Mail empfangen wurde, usw.), ohne dafür eine spezielle Untersuchungsaufgabe zu erstellen. Das zu untersuchende Objekt kann aus dem Interface von Kaspersky Internet Security 6.0 oder mit den Standardmitteln von Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) ausgewählt werden.

Eine vollständige Liste der Aufgaben zur Virensuche, die für Ihren Computer erstellt wurden, kann im Abschnitt **Virensuche** auf der linken Seite des Programmhauptfensters angezeigt werden.

14.1. Steuerung von Aufgaben zur Virensuche

Der Start von Aufgaben zur Virensuche erfolgt entweder manuell oder automatisch nach einem festgelegten Zeitplan (s. Pkt. 6.5 auf S. 91).

Um eine Untersuchungsaufgabe manuell zu starten,

> wählen Sie im Abschnitt **Virensuche** des Programmhauptfensters den Aufgabennamen und klicken Sie in der Statuszeile auf die Schaltfläche ▶.
>
> Momentan ausgeführte Aufgaben werden im Kontextmenü angezeigt, das durch Rechtsklick auf das Anwendungssymbol in der Taskleiste geöffnet wird.

Um die Ausführung einer Aufgabe anzuhalten,

> klicken Sie in der Statuszeile auf die Schaltfläche ❚❚. Dabei ändert sich der Status der Aufgabenausführung in *Pause*. Die Untersuchung wird angehalten, bis die Aufgabe manuell oder nach Zeitplan erneut gestartet wird.

Um die Ausführung einer Aufgabe zu beenden,

> klicken Sie in der Statuszeile auf die Schaltfläche ■. Der Status der Aufgabenausführung ändert sich in *abgebrochen*. Die Untersuchung wird angehalten, bis die Aufgabe manuell oder nach Zeitplan erneut gestartet wird. Beim folgenden Start der Aufgabe wird Ihnen vorgeschlagen, die abgebrochene Untersuchung fortzusetzen oder erneut zu beginnen.

14.2. Erstellen einer Liste der Untersuchungsobjekte

Um eine Liste der Objekte anzuzeigen, die bei der Ausführung dieser Aufgabe untersucht werden, wählen Sie im Abschnitt **Virensuche** des Programmhauptfensters den Namen einer Aufgabe (z.B. **Arbeitsplatz**). Die Liste der Objekte wird auf der rechten Seite des Fensters unter der Statuszeile angezeigt (s. Abb. 64).

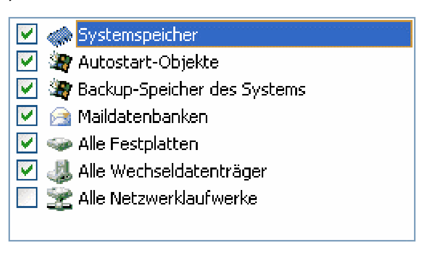


Abbildung 64. Liste der Untersuchungsobjekte

Für Aufgaben, die standardmäßig bei der Programminstallation erstellt wurden, besteht bereits eine Liste der zu untersuchenden Objekte. Beim Erstellen eigener Aufgaben oder bei der Auswahl eines Objekts im Rahmen einer Aufgabe zur Virenuntersuchung eines separaten Objekts erstellen Sie die Liste der Objekte selbst.

Zum Ergänzen und Ändern der Liste der Untersuchungsobjekte dienen die Schaltflächen, die rechts von der Liste angebracht sind. Klicken Sie auf die Schaltfläche **Hinzufügen**, um der Liste ein neues Untersuchungsobjekt hinzuzufügen und geben Sie im folgenden Fenster das Untersuchungsobjekt an.

Aus Gründen der Bedienungsfreundlichkeit können dem Untersuchungsbereich solche Kategorien wie Maildatenbanken, Systemspeicher, Autostart-Objekte, Sicherungsdateien des Betriebssystems, und Objekte, die sich im Quarantäne-ordner von Kaspersky Internet Security befinden, hinzugefügt werden.

Außerdem kann beim Hinzufügen eines Ordners, der untergeordnete Objekte enthält, die Option zur rekursiven Untersuchung geändert werden. Verwenden Sie dazu den entsprechenden Punkt des Kontextmenüs.

Um ein Objekt zu löschen, markieren Sie es in der Liste (dabei wird der Objektname durch grauen Hintergrund hervorgehoben) und klicken Sie auf die Schaltfläche **Löschen**. Sie können die Untersuchung einzelner Objekte bei der Ausführung einer bestimmten Aufgabe vorübergehend abschalten, ohne die Objekte aus der Liste zu löschen. Deaktivieren Sie dazu einfach das Kontrollkästchen neben dem Objekt, das nicht untersucht werden soll.

Klicken Sie zum Starten einer Untersuchungsaufgabe auf die Schaltfläche **Virensuche** oder wählen Sie im Menü, das durch Klick auf die Schaltfläche **Aktionen** geöffnet wird, den Punkt **Start**.

Außerdem können Sie ein Untersuchungsobjekt mit den Standardmitteln des Betriebssystems Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) auswählen (s. Abb. 65). Führen Sie dazu den Mauszeiger auf den Namen des gewünschten Objekts, öffnen Sie mit der rechten Maustaste das Microsoft Windows-Kontextmenü und wählen Sie den Punkt **Auf Viren untersuchen**.

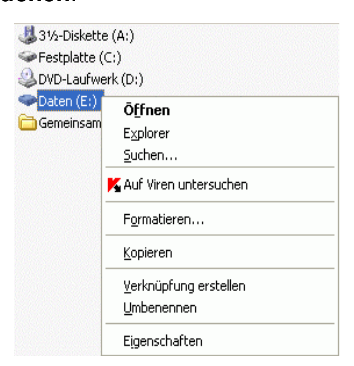


Abbildung 65. Untersuchung eines Objekts aus dem Kontextmenü von Microsoft Windows

14.3. Erstellen von Aufgaben zur Virensuche

Zur Virenuntersuchung von Objekten Ihres Computers können Sie die vordefinierten Untersuchungsaufgaben verwenden, die zum Lieferumfang des Programms gehören, sowie eigene Aufgaben erstellen. Eine neue Aufgabe wird auf der Basis von bereits vorhandenen Untersuchungsaufgaben erstellt.

Um eine neue Untersuchungsaufgabe zu erstellen,

1. Wählen Sie im Abschnitt **Virensuche** des Programmhauptfensters die Aufgabe, deren Parameter Ihren Anforderungen am nächsten kommen.

2. Öffnen Sie durch Rechtsklick das Kontextmenü oder klicken Sie auf die Schaltfläche **Aktionen**, die sich rechts neben der Liste der Untersuchungsobjekte befindet, und wählen Sie den Punkt **Speichern unter**.

3. Geben Sie im folgenden Fenster den Namen der neuen Aufgabe an und klicken Sie auf die Schaltfläche **OK**. Danach erscheint die Aufgabe

mit dem festgelegten Namen in der Aufgabenliste des Abschnitts **Virensuche** im Programmhauptfenster.

> Achtung!
>
> Der Benutzer kann maximal vier Aufgaben erstellen.

Eine neu erstellte Aufgabe erbt alle Parameter der Aufgabe, auf deren Basis sie erstellt wurde. Deshalb ist die zusätzliche Konfiguration erforderlich: Erstellen Sie eine Liste der Untersuchungsobjekte (s. Pkt. 14.2 auf S. 223), legen Sie die Parameter fest (s. Pkt. 14.4 auf S. 226), mit denen die Aufgabe ausgeführt werden soll, und erstellen Sie den Zeitplan (s. Pkt. 6.5 auf S. 91) für den automatischen Start.

Um eine Aufgabe umzubenennen,

wählen Sie die Aufgabe im Abschnitt **Virensuche** des Programmhauptfensters, öffnen Sie durch Rechtsklick das Kontextmenü oder klicken Sie auf die Schaltfläche **Aktionen**, die sich rechts neben der Liste der Untersuchungsobjekte befindet, und wählen Sie den Punkt **Umbenennen**.

Geben Sie im folgenden Fenster den neuen Namen für die Aufgabe an und klicken Sie auf die Schaltfläche **OK**. Dadurch wird der Aufgabenname im Abschnitt **Virensuche** geändert.

Um eine Aufgabe zu löschen,

wählen Sie die Aufgabe im Abschnitt **Virensuche** des Programmhauptfensters, öffnen Sie durch Rechtsklick das Kontextmenü oder klicken Sie auf die Schaltfläche **Aktionen**, die sich rechts neben der Liste der Untersuchungsobjekte befindet, und wählen Sie den Punkt **Löschen**.

Bestätigen Sie im Bestätigungsfenster, dass die Aufgabe gelöscht werden soll. Dadurch wird die Aufgabe aus der Aufgabenliste im Abschnitt **Virensuche** gelöscht.

> Achtung!
>
> Nur Aufgaben, die von Ihnen selbst erstellt wurden, können umbenannt und gelöscht werden.

14.4. Konfiguration von Aufgaben zur Virensuche

Auf welche Weise die Untersuchung von Objekten auf Ihrem Computer erfolgt, wird durch eine Auswahl von Parametern bestimmt, die für jede Aufgabe festgelegt werden.

Um zur Konfiguration der Aufgabenparameter zu wechseln,

wählen Sie den Namen der Aufgabe im Abschnitt **Virensuche** des Hauptfensters und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Aufgabe.

Im Konfigurationsfenster können Sie für jede der Aufgaben:

- die Sicherheitsstufe wählen, auf deren Basis die Aufgabe ausgeführt werden soll (s. Pkt. 14.4.1 auf S. 227).
- zur detaillierten Konfiguration der Stufe wechseln:
    - die Parameter angeben, welche die Dateitypen bestimmen, die der Virusanalyse unterzogen werden (s. Pkt. 14.4.2 auf S. 228).
    - den Start von Aufgaben unter einem anderen Benutzerkonto konfigurieren (s. Pkt. 6.4 auf S. 89).
    - zusätzliche Parameter für die Untersuchung angeben (s. Pkt. 14.4.5 auf S. 234).
- die standardmäßig verwendeten Untersuchungsparameter wiederherstellen (s. Pkt. 14.4.3 auf S. 231).
- die Aktion wählen, die vom Programm beim Fund eines infizierten bzw. möglicherweise infizierten Objekts angewandt wird (s. Pkt. 14.4.4 auf S. 232).
- einen Zeitplan für den automatischen Aufgabenstart erstellen (s. Pkt. 6.5 auf S. 91).

Außerdem können Sie einheitliche Parameter für den Start aller Aufgaben festlegen (s. Pkt. 14.4.6 auf S. 236).

Im Folgenden werden alle oben aufgezählten Parameter zur Konfiguration einer Aufgabe ausführlich beschrieben.

14.4.1. Auswahl der Sicherheitsstufe

Jede Aufgabe zur Virensuche gewährleistet die Untersuchung von Objekten auf einer der folgenden Stufen (s. Abb. 66):

Hoch – Untersuchung des gesamten Computers oder eines Laufwerks, Ordners oder einer Datei mit maximaler Ausführlichkeit. Die Verwendung dieser Stufe wird empfohlen, wenn der Verdacht auf eine Virusinfektion Ihres Computers besteht.

Empfohlen - Die Parameter dieser Stufe entsprechen den von den Kaspersky-Lab-Experten empfohlenen Einstellungen. Sie umfassen die Untersuchung der gleichen Objekte wie bei der Stufe **Hoch** unter Ausnahme von Dateien in Mailformaten.

Niedrig – Da die Auswahl der untersuchten Dateien auf dieser Stufe eingeschränkt wird, erlaubt Ihnen diese Stufe, komfortabel mit Anwendungen zu arbeiten, die den Arbeitsspeicher stark beanspruchen.

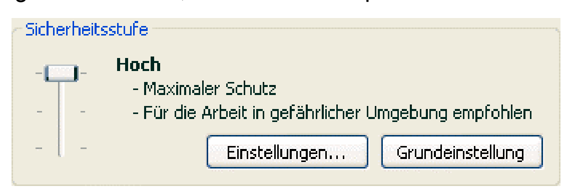


Abbildung 66. Auswahl der Sicherheitsstufe für die Virenuntersuchung von Objekten

Die Untersuchung von Objekten erfolgt standardmäßig auf der **Empfohlenen** Stufe.

Sie können die Stufe für die Untersuchung von Dateien erhöhen oder senken, indem Sie eine andere Stufe wählen oder die Einstellungen der aktuellen Stufe ändern.

Um die Sicherheitsstufe zu ändern,

verschieben Sie den Zeiger auf der Skala. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Dateien bestimmt: Je weniger Dateien der Virusanalyse unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn keine der genannten Sicherheitsstufen für die Untersuchung Ihren Anforderungen entspricht, können Sie die Untersuchungsparameter zusätzlich anpassen. Wählen Sie dazu die Stufe, die Ihren Anforderungen am nächsten kommt, als Ausgangsstufe und ändern Sie ihre Parameter entsprechend. In diesem Fall ändert sich die Stufe in **Benutzerdefiniert**.

Um die Einstellungen der aktuellen Sicherheitsstufe anzupassen,

klicken Sie im Konfigurationsfenster der Aufgabe auf die Schaltfläche **Einstellungen**, passen im folgenden Fenster die Einstellungen für die Untersuchung an und klicken auf die Schaltfläche **OK**.

Dadurch wird eine vierte Sicherheitsstufe mit der Bezeichnung **Benutzerdefiniert** erstellt, welche die von Ihnen definierten Untersuchungsparameter enthält.

14.4.2. Festlegen der zu untersuchenden Objekttypen

Durch die Angabe der Typen der zu untersuchenden Objekte bestimmen Sie das Format, die Größe und die Laufwerke der Dateien die beim Ausführen dieser Aufgabe untersucht werden sollen.

Der Typ der zu untersuchenden Dateien wird im Abschnitt **Dateitypen** festgelegt (s. Abb. 67). Wählen Sie eine der drei Varianten:

- **Alle Dateien untersuchen**. In diesem Fall werden alle Dateien ohne Ausnahme der Untersuchung unterzogen.
- **Programme und Dokumente (nach Inhalt) untersuchen**. Bei der Auswahl dieser Gruppe untersucht das Programm nur potentiell infizierbare Dateien, d.h. Dateien, in die ein Virus eindringen kann.

  > Hinweis.
  >
  > Es gibt eine Reihe von Dateiformaten, für die das Risiko des Eindringens von schädlichem Code und der späteren Aktivierung relativ gering ist. Dazu zählen beispielsweise Dateien im *txt*-Format.
  >
  > Im Gegensatz dazu gibt es Dateiformate, die ausführbaren Code enthalten oder enthalten können. Als Beispiele für solche Objekte dienen Dateien der Formate *exe*, *dll*, *doc*. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

  Bevor die Virensuche in einem Objekt beginnt, wird die interne Kopfzeile des Objekts hinsichtlich des Dateiformats analysiert (txt, doc, exe usw.).

- **Programme und Dokumente (nach Erweiterung) untersuchen**. In diesem Fall untersucht das Programm nur potentiell infizierbare Dateien, wobei das Dateiformat auf Basis der Dateinamenserweiterung ermittelt wird. Wenn Sie dem Link Erweiterung folgen, gelangen Sie zu einer Liste der Dateierweiterungen, die in diesem Fall untersucht werden (s. Anhang A.1 auf S. 329).

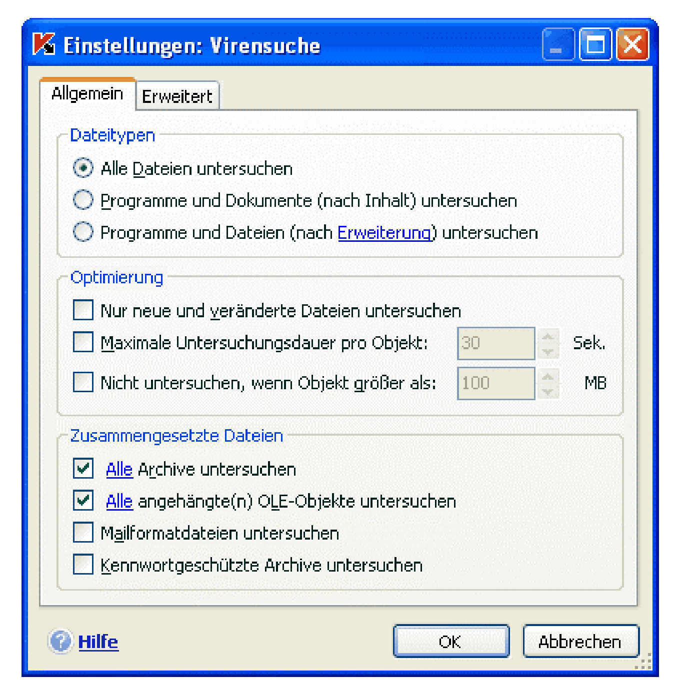


Abbildung 67. Untersuchungseinstellungen

Hinweis.

Es sollte beachtet werden, dass ein Angreifer einen Virus in einer Datei mit der Erweiterung txt an Ihren Computer senden kann, obwohl es sich in Wirklichkeit um eine ausführbare Datei handelt, die in eine txt-Datei umbenannt wurde. Wenn Sie die Variante **Programme und Dokumente (nach Erweiterung) untersuchen** wählen, wird eine solche Datei bei der Untersuchung übersprungen. Wenn Sie die Variante **Programme und Dokumente (nach Inhalt) untersuchen** gewählt haben, analysiert das Programm ungeachtet der Erweiterung die Kopfzeile der Datei, wodurch sich ergibt, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Im Abschnitt **Optimierung** lässt sich festlegen, dass nur Dateien untersucht werden sollen, die neu sind oder seit ihrer letzten Analyse verändert wurden. Dieser Modus erlaubt es, die Untersuchungszeit wesentlich zu verkürzen und die Arbeitsgeschwindigkeit des Programms zu erhöhen. Aktivieren Sie dazu das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**. Dieser Modus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Geben Sie im Abschnitt **Zusammengesetzte Dateien** an, welche zusammengesetzten Dateien auf Viren untersucht werden sollen:

Außerdem kann im Abschnitt **Optimierung** eine Begrenzung für die Untersuchungszeit und die maximale Größe eines einzelnen Objekts festgelegt werden.

- ☑ **Maximale Untersuchungsdauer pro Objekt ... Sek**. Aktivieren Sie das Kontrollkästchen, um die Untersuchung eines einzelnen Objekts in zeitlicher Hinsicht zu begrenzen, und geben Sie die maximale Untersuchungsdauer für ein Objekt im Feld rechts an. Bei einer Überschreitung der Zeitbegrenzung wird das Objekt von der Untersuchung ausgeschlossen.
- ☑ **Nicht untersuchen, wenn Objekt größer als ... MB**. Aktivieren Sie das Kontrollkästchen, um die Untersuchung eines einzelnen Objekts hinsichtlich der Größe zu begrenzen, und geben Sie die maximal zulässige Größe eines Objekts im Feld rechts an. Bei einer Überschreitung der Größenbegrenzung wird das Objekt von der Untersuchung ausgeschlossen.

Geben Sie im Abschnitt **Zusammengesetzte Dateien** an, welche zusammengesetzten Dateien auf Viren analysiert werden sollen:

- ☑ **Alle/Nur neue Archive untersuchen** – Archive der Formate RAR, ARJ, ZIP, CAB, LHA, JAR, ICE untersuchen.

> Achtung!
>
> Archive, in denen Kaspersky Internet Security die Desinfektion nicht unterstützt (z.B. HA, UUE, TAR), werden nicht automatisch gelöscht, selbst wenn als Aktion die automatische Desinfektion oder das Löschen irreparabler Objekte gewählt wurde.
>
> Verwenden den Link Archiv löschen im Meldungsfenster über den Fund des gefährlichen Objekts, um solche Archive zu löschen. Diese Meldung erscheint auf dem Bildschirm, nachdem die Bearbeitung von während der Untersuchung gefundenen Objekten gestartet wurde. Außerdem kann ein infiziertes Archiv auch manuell aus dem Computer entfernt werden.

- ☑ **Alle/Nur neue angehängte(n) OLE-Objekte untersuchen** – Objekte, die in eine Datei eingebettet sind, untersuchen (beispielsweise eine Excel-Tabelle oder ein Makro, das in eine Microsoft Word-Datei eingebettet ist, der Anhang einer E-Mail-Nachricht, usw.).

Für jeden Typ einer zusammengesetzten Datei können Sie wählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie dazu den Link neben der Bezeichnung des Objekts. Der Link verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn im Abschnitt **Optimierung** festgelegt wurde, dass nur neue und veränderte Dateien untersucht werden sollen, steht die Auswahl des Typs der zusammengesetzten Dateien nicht zur Verfügung.

 **Mailformatdateien untersuchen** – Dateien in Mailformaten und Maildatenbanken untersuchen. Wenn das Kontrollkästchen aktiviert ist, zerlegt Kaspersky Internet Security eine Mailformatdatei und analysiert jede Komponente der E-Mail (Briefkörper, Anhang) auf Viren. Wenn das Kontrollkästchen nicht angekreuzt ist, wird die Mailformatdatei als einheitliches Objekt untersucht.

Beachten Sie folgende Besonderheiten bei der Untersuchung von Maildatenbanken, die durch Kennwort geschützt sind:

- Kaspersky Internet Security erkennt schädlichen Code in Datenbanken für Microsoft Office Outlook 2000, desinfiziert diesen aber nicht.
- Das Programm unterstützt die Suche nach schädlichem Code in geschützten Maildatenbanken für Microsoft Office Outlook 2003 nicht.

Kennwortgeschützte Archive untersuchen – Untersuchung von Archiven, die durch Kennwort geschützt sind. In diesem Fall erfolgt vor der Untersuchung von Objekten, die in dem Archiv enthalten sind, auf dem Bildschirm eine Kennwortabfrage. Wenn das Kontrollkästchen nicht aktiviert ist, werden kennwortgeschützte Archive bei der Untersuchung übersprungen.

14.4.3. Wiederherstellen der standardmäßigen Untersuchungseinstellungen

Während der Konfiguration der Parameter für die Aufgabenausführung können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Untersuchungseinstellungen für Objekte wiederherzustellen,

1. Wählen Sie den Namen der Datei im Abschnitt **Virensuche** des Hauptfensters und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Aufgabe.
2. Klicken Sie im Abschnitt **Sicherheitsstufe** auf die Schaltfläche **Grundeinstellung**.

14.4.4. Auswahl der Aktion für Objekte

Wenn sich durch die Virenuntersuchung eines Objekts herausstellt, dass es infiziert oder verdächtig ist, hängen die weiteren Operationen des Programms vom Status des Objekts und von der ausgewählten Aktion ab.

Ein Objekt kann aufgrund der Untersuchung einen der folgenden Status erhalten:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise wurde in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden.

Standardmäßig werden alle infizierten Dateien der Desinfektion unterzogen und alle möglicherweise infizierten Dateien in die Quarantäne verschoben.

Um die Aktion für ein Objekt zu ändern,

wählen Sie den Namen der Aufgabe im Abschnitt **Virensuche** des Programmhauptfensters und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Aufgabe. Alle verfügbaren Aktionen werden im entsprechenden Abschnitt genannt (s. Abb. 68).

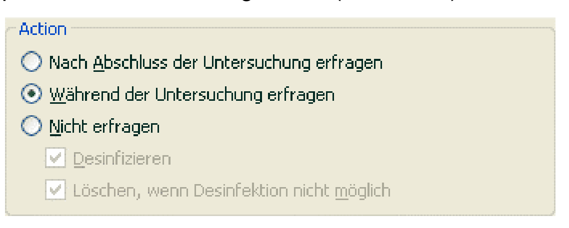


Abbildung 68. Auswahl der Aktion für ein gefährliches Objekt

Gewählte Aktion	Was geschieht beim Fund eines infizierten/ möglicherweise infizierten Objekts?
Nach Abschluss der Untersuchung erfragen	Das Programm schiebt die Bearbeitung von Objekten bis zum Ende der Untersuchung auf. Nach dem Abschluss der Untersuchung erscheint auf dem Bildschirm ein Statistik-Fenster mit einer Liste der gefundenen Objekte und Ihnen wird angeboten, die Objektbearbeitung durchzuführen.
Während der Untersuchung erfragen	Das Programm zeigt eine Warn-meldung auf dem Bildschirm an, die Informationen darüber enthält, von welchem schädlichen Code das Objekt infiziert/möglicherweise infiziert ist, und bietet Aktionen zur Auswahl an.
Nicht erfragen	Das Programm protokolliert im Bericht Informationen über die gefundenen Objekte. Die Objekte werden nicht bearbeitet und der Benutzer wird nicht benachrichtigt. Es wird davor gewarnt, diesen Funktionsmodus für das Programm zu wählen, weil infizierte und möglicherweise infizierte Objekte dann auf Ihrem Computer verbleiben und es praktisch unmöglich ist, eine Infektion zu verhindern.

Nicht erfragen **Desinfizieren**	Das Programm führt einen Desinfektionsversuch mit dem gefundenen Objekt aus, ohne nach der Bestätigung des Benutzers zu fragen. Wenn der Desinfektionsversuch erfolglos bleibt, erhält das Objekt den Status *möglicherweise infiziert* und wird in die Quarantäne verschoben (s. Pkt. 17.1 auf S. 258). Informationen darüber werden im Bericht aufgezeichnet (s. Pkt. 17.3 auf S. 265). Später kann versucht werden, das Objekt zu desinfizieren.
Nicht erfragen **Desinfizieren** **Löschen, wenn Desinfektion nicht möglich**	Das Programm führt einen Desinfektionsversuch mit dem gefundenen Objekt aus, ohne nach der Bestätigung des Benutzers zu fragen. Wenn der Desinfektionsversuch erfolglos bleibt, wird das Objekt gelöscht.
Nicht erfragen **Desinfizieren** **Löschen**	Das Programm löscht das Objekt automatisch.

Bevor ein Desinfektionsversuch erfolgt oder das Objekt gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an und speichert diese im Backup (s. Pkt. 17.2 auf S. 262). Dadurch wird ermöglicht, das Objekt bei Bedarf wiederherzustellen oder möglicherweise später zu desinfizieren.

14.4.5. Zusätzliche Optionen für die Virensuche

Neben der Konfiguration der grundlegenden Parameter für die Virenuntersuchung können Sie noch zusätzliche Parameter festlegen (s. Abb. 69):

iChecker-Technologie aktivieren – Die Verwendung dieser Technologie erlaubt eine Steigerung der Untersuchungsgeschwindigkeit, weil bestimmte Objekte von der Untersuchung ausgeschlossen werden. Das Ausschließen eines Objekts von der Untersuchung erfolgt nach einem speziellen Algorithmus, der das Erscheinungsdatum der Bedrohungssignaturen, das

Datum der letzten Untersuchung des Objekts und die Änderung von Untersuchungseinstellungen berücksichtigt.

Wurde beispielsweise eine Archivdatei vom Programm untersucht und ihr wurde der Status virusfrei zugewiesen, dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn Sie die Zusammensetzung des Archivs durch das Hinzufügen eines neuen Objekts verändert, die Untersuchungsparameter geändert haben, oder wenn die Datenbanken für die Bedrohungssignaturen aktualisiert wurden, wird das Archiv erneut untersucht.

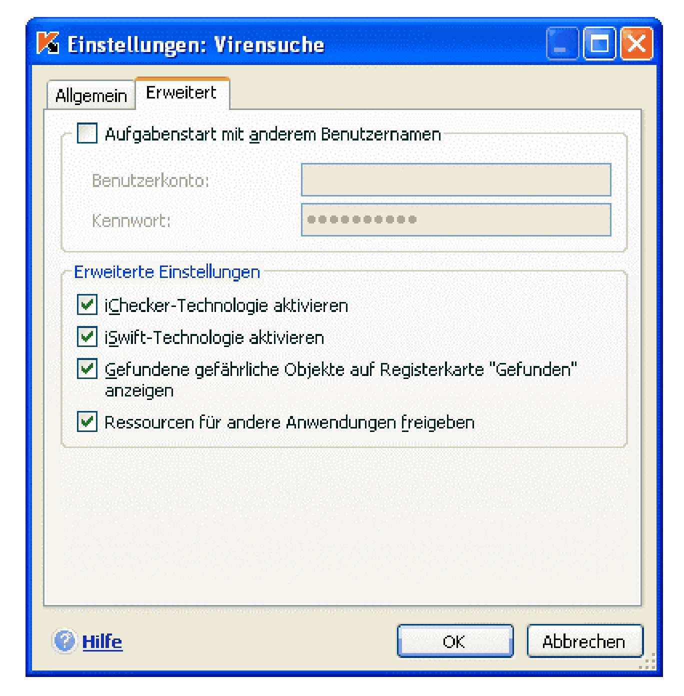


Abbildung 69. Erweiterte Untersuchungseinstellungen

Die Technologie iChecker™ besitzt Einschränkungen: Sie funktioniert nicht mit großen Dateien und kann nur auf Objekte angewandt werden, deren Struktur der Anwendung Kaspersky Internet Security bekannt ist (z.B. die Dateiformate *exe*, *dll*, *lnk*, *ttf*, *inf*, *sys*, *com*, *chm*, *zip*, *rar*).

☑ **iSwift-Technologie aktivieren** – Diese Technologie stellt eine Weiterentwicklung der iChecker-Technologie für Computer mit NTSF-Dateisystem dar. Die Technologie iSwift besitzt folgende Einschränkungen: Sie ist an einen konkreten Ort der Datei im Dateisystem gebunden und kann

nur auf Objekte angewandt werden, die sich in einem NTFS-Dateisystem befinden.

> Die iSwift-Technologie steht auf Computern mit dem Betriebssystem Microsoft Windows 98SE/ME/XP64 nicht zur Verfügung.

☑ **Gefundene gefährliche Objekte auf Registerkarte "Gefunden" anzeigen** – Eine Liste der bei der Untersuchung gefundenen Bedrohungen auf der Registerkarte **Gefunden** im Berichtsfenster anzeigen (s. Pkt. 17.3.2 auf S. 269). Das Deaktivieren dieser Funktion kann bei speziellen Untersuchungen von Nutzen sein, beispielsweise zur Erhöhung der Geschwindigkeit bei der Untersuchung einer Testsammlung.

☑ **Ressourcen für andere Anwendungen freigeben** – Die Ausführung dieser Untersuchungsaufgabe anhalten, wenn die Prozessorressourcen von anderen Anwendungen beansprucht werden.

14.4.6. Festlegen einheitlicher Untersuchungsparameter für alle Aufgaben

Jede Untersuchungsaufgabe wird mit eigenen Parametern ausgeführt. Für die Aufgaben, die bei der Programminstallation auf dem Computer erstellt wurden, gelten standardmäßig die von den Kaspersky-Lab-Spezialisten empfohlenen Parameter.

Sie können einheitliche Untersuchungsparameter für alle Aufgaben festlegen. Als Grundlage gilt dabei die Auswahl der Parameter, die bei der Virenuntersuchung eines einzelnen Objekts verwendet werden.

Um einheitliche Untersuchungsparameter für alle Aufgaben festzulegen:

1. Wählen Sie den Abschnitt **Virensuche** auf der linken Seite des Programmhauptfensters und verwenden Sie den Link Einstellungen.

2. Legen Sie im folgenden Konfigurationsfenster die Untersuchungsparameter fest: Wählen Sie die Sicherheitsstufe (s. Pkt. 14.4.1 auf S. 227), nehmen Sie die erweiterten Einstellungen für die Sicherheitsstufe vor und bestimmen Sie die Aktion für Objekte (s. Pkt. 14.4.4 auf S. 232).

3. Klicken Sie auf die Schaltfläche **Übernehmen** im Abschnitt **Einstellungen anderer Aufgaben**, um die vorgenommenen Änderungen für alle Aufgaben zu übernehmen. Bestätigen Sie das Festlegen der einheitlichen Parameter.

KAPITEL 15. TESTEN DER ARBEIT VON KASPERSKY INTERNET SECURITY

Nach Installation und Konfiguration von Kaspersky Internet Security wird empfohlen, die Korrektheit von Einstellungen und Funktion der Anwendung mit Hilfe eines "Testvirus" und seinen Modifikationen zu prüfen.

15.1. EICAR-"Testvirus" und seine Modifikationen

Dieser Testvirus wurde vom Institut eicar (The European Institute for Computer Antivirus Research) speziell zum Überprüfen der Arbeit von Antivirenprodukten entwickelt.

Der "Testvirus" IST KEIN VIRUS und enthält keinen Programmcode, der Ihren Rechner beschädigen könnte. Trotzdem wird er von den meisten Antiviren-Softwareprodukten als Virus erkannt.

> Verwenden Sie nie echte Viren, um die Funktionsfähigkeit eines Antivirenprodukts zu testen!

Der "Testvirus" kann von der offiziellen Internetseite des **EICAR**-Instituts heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm.

Die von der Webseite des **EICAR**-Instituts heruntergeladene Datei enthält den Code des standardmäßigen "Testvirus". Kaspersky Internet Security erkennt diese Datei, weist ihr den Typ **Virus** zu und führt die für diesen Objekttyp festgelegte Aktion aus.

Um die Reaktion von Kaspersky Internet Security beim Fund von Objekten eines anderen Typs zu prüfen, können Sie den Inhalt des standardmäßigen "Testvirus" durch Hinzufügen eines Präfixes modifizieren (s. Tabelle).

Präfix	Status des "Testvirus"	Entsprechende Aktion bei der Bearbeitung des Objekts durch die Anwendung
kein Präfix, standard-mäßiger "Testvirus"	Die Datei enthält den "Testvirus". Die Desinfektion ist nicht möglich.	Die Anwendung identifiziert dieses Objekt als schädlich und irreparabel. Das Objekt wird gelöscht.
CORR–	Beschädigt.	Die Anwendung hat Zugriff auf das Objekt erhalten, kann es aber nicht untersuchen, weil es beschädigt ist (z.B. Struktur des Objekts ist beschädigt, ungültiges Dateiformat).
SUSP– WARN–	Die Datei enthält den "Testvirus" (Modifikation). Die Desinfektion ist nicht möglich.	Dieses Objekt ist eine Modifikation eines bekannten oder unbekannten Virus. Im Moment des Funds enthalten die Datenbanken mit den Bedrohungssignaturen keine Beschreibung zur Desinfektion dieses Objekts. Die Anwendung verschiebt das Objekt in die Quarantäne, um es später mit aktualisierten Bedrohungs-signaturen zu bearbeiten.
ERRO–	Bearbeitungsfehler.	Während der Bearbeitung des Objekts ist ein Fehler aufgetreten: Die Anwendung erhält keinen Zugriff auf das Untersuchungs-objekt, weil die Integrität des Objekts beschädigt ist (z.B. kein Endpunkt in einem Multi-Level-Archiv) oder die Verbindung zu dem Objekt fehlt (wenn ein Objekt in einer Netzwerkressource untersucht wird).

Präfix	Status des "Testvirus"	Entsprechende Aktion bei der Bearbeitung des Objekts durch die Anwendung
CURE-	Die Datei enthält den "Testvirus". Die Desinfektion ist möglich. Das Objekt kann repariert werden, wobei der Text des "Viruskörpers" in CURE geändert wird.	Das Objekt enthält einen Virus, der desinfiziert werden kann. Die Anwendung führt die Antivirenbearbeitung des Objekts durch. Danach ist das Objekt vollständig repariert.
DELE-	Die Datei enthält den "Testvirus". Die Desinfektion ist nicht möglich.	Dieses Objekt ist irreparabel von einem Virus infiziert oder ist ein trojanisches Programm. Die Anwendung löscht solche Objekte.

Die erste Spalte der Tabelle enthält Präfixe, die dem standardmäßigen "Testvirus" am Zeilenanfang hinzugefügt werden können. In der zweiten Spalte werden für die unterschiedlichen Typen des "Testvirus" der Status und die Reaktion von Kaspersky Internet Security beschrieben. Die dritte Spalte bietet Informationen über die vom Status abhängige Bearbeitung der Objekte durch die Anwendung.

Die Aktionen für das jeweilige Objekt werden durch die vorgegebenen Einstellungen für die Antivirenuntersuchung festgelegt.

15.2. Testen des Datei-Anti-Virus

Um die Funktionsfähigkeit von Datei-Anti-Virus zu testen:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen EICAR-Seite (s. Pkt. 15.1 auf S. 237) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.

2. Erlauben Sie das Protokollieren aller Ereignisse im Bericht, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden. Aktivieren Sie dazu im Konfigurationsfenster für Berichte das Kontrollkästchen ☑ **Informative Ereignisse protokollieren** (s. Pkt. 17.3.1 auf S. 268).

3. Starten Sie den "Testvirus" oder seine Modifikation zur Ausführung.

Datei-Anti-Virus fängt den Zugriff auf die Datei ab, untersucht sie und benachrichtigt Sie über den Fund eines gefährlichen Objekts:



Abbildung 70. Ein gefährliches Objekt wurde gefunden

Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Reaktion von Datei-Anti-Virus auf den Fund verschiedener Objekttypen testen.

Das vollständige Arbeitsergebnis von Datei-Anti-Virus ist im Bericht über die Arbeit der Komponente enthalten.

15.3. Testen einer Aufgabe zur Virensuche

Um eine Untersuchungsaufgabe zu testen:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen EICAR-Seite (s. Pkt. 15.1 auf S. 237) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.

2. Erstellen Sie eine neue Aufgabe (s. Pkt. 14.3 auf S. 224) zur Virensuche und wählen Sie als Untersuchungsobjekt den Ordner (s. Pkt. 15.1 auf S. 237), der die "Testviren" enthält.
3. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht wurden, in der Berichtsdatei gespeichert werden. Aktivieren Sie dazu im Konfigurationsfenster für Berichte das Kontrollkästchen ☑ **Informative Ereignisse protokollieren**.
4. Starten Sie die Ausführung der Aufgabe zur Virensuche (s. Pkt. 14.1 auf S. 222).

Während der Untersuchung werden beim Fund verdächtiger oder infizierter Objekte auf dem Bildschirm Meldungen mit Informationen über das Objekt und einer Bestätigungsabfrage zur folgenden Aktion angezeigt:



Abbildung 71. Ein gefährliches Objekt wurde gefunden

Durch die Auswahl unterschiedlicher Aktionsvarianten können Sie die Reaktion von Kaspersky Internet Security auf den Fund der einzelnen Objekttypen testen.

Das vollständige Arbeitsergebnis der Ausführung der Untersuchungsaufgabe ist im Bericht über die Arbeit der Komponente enthalten.

KAPITEL 16. UPDATE DES PROGRAMMS

Eine Voraussetzung für die Sicherheit Ihres Computers ist die Pflege des aktuellen Zustands von Kaspersky Internet Security. Jeden Tag tauchen neue Viren, Trojaner und andere schädliche Programme auf. Deshalb ist es sehr wichtig sicherzustellen, dass Ihre Informationen zuverlässig geschützt werden.

Die Aktualisierung des Programms umfasst den Download und die Installation folgender Elemente auf Ihren Computer:

- **Bedrohungssignaturen, Angriffssignaturen und Netzwerktreiber**

  Der Schutz der Informationen auf ihrem Computer basiert auf Datenbanken, die Bedrohungssignaturen und Beschreibungen von Netzwerkangriffen enthalten. Die Schutzkomponenten verwenden diese bei der Suche und Desinfektion gefährlicher Objekte auf Ihrem Computer. Die Signaturen werden stündlich durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird ausdrücklich empfohlen, die Signaturen regelmäßig zu aktualisieren.

  Gemeinsam mit den Bedrohungssignaturen und der Datenbank über Netzwerkangriffe werden auch die Netzwerktreiber aktualisiert, die die Funktionalität für das Abfangen des Netzwerkverkehrs durch die Schutzkomponenten gewährleisten.

  In den vorhergehenden Versionen der Antiviren-Anwendungen von Kaspersky Lab wurde die Arbeit mit einer unterschiedlichen Auswahl von Bedrohungssignaturen unterstützt: *Standard*- oder *erweiterte Auswahl*. Sie unterschieden sich im Hinblick auf die Typen der gefährlichen Objekte, vor denen Sie Ihren Computer schützten. In Kaspersky Internet Security 6.0 brauchen Sie sich nicht um die Auswahl der passenden Art von Bedrohungssignaturen kümmern. Bei der Arbeit unserer Produkte werden jetzt Bedrohungssignaturen verwendet, die nicht nur den Schutz vor unterschiedlichen Arten schädlicher und potentiell gefährlicher Objekte, sondern auch vor Hackerangriffen bieten.

- **Programm-Module**

  Neben den Bedrohungssignaturen können Sie auch die Programm-Module von Kaspersky Internet Security aktualisieren. Kaspersky Lab gibt periodisch Updatepakete heraus.

Als primäre Updatequelle für Kaspersky Internet Security dienen u.a. folgende Updateserver von Kaspersky Lab:

http://downloads1.kaspersky-labs.com/updates/
http://downloads2.kaspersky-labs.com/updates/
ftp://downloads1.kaspersky-labs.com/updates/

Für den erfolgreichen Updatedownload von den Servern ist eine Verbindung Ihres Computers mit dem Internet erforderlich.

Der Updatedownload erfolgt in einem der folgenden Modi:

- *Automatisch*. Kaspersky Internet Security prüft in festgelegten Zeitabständen, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Virusepidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates vorhanden sind, lädt die Anwendung sie herunter und installiert sie auf dem Computer. Dieser Modus gilt als Standard.
- *Nach Zeitplan*. Die Aktualisierung des Programms erfolgt nach einem festgelegten Zeitplan.
- *Manuell*. In diesem Fall starten Sie die Aktualisierung des Programms selbständig.

Beim Updatevorgang werden die Programm-Module und die Bedrohungssignaturen auf Ihrem Computer mit den auf der Updatequelle vorhandenen verglichen. Wenn auf Ihrem Computer die aktuelle Version der Signaturen und Module installiert ist, erscheint auf dem Bildschirm eine Meldung über die Aktualität des Schutzes auf Ihrem Computer. Wenn Signaturen und Module nicht aktuell sind, wird nur der fehlende Teil der Updates auf Ihrem Computer installiert. Signaturen und Module werden nicht vollständig kopiert, wodurch die Updategeschwindigkeit wesentlich gesteigert und der Netzwerkverkehr entlastet wird.

Bevor die Bedrohungssignaturen aktualisiert werden, legt Kaspersky Internet Security eine Sicherungskopie davon an. Bei Bedarf können Sie zu den vorhergehenden Signaturen zurückkehren.

Die Möglichkeit der Rückkehr (s. Pkt. 16.2 auf S. 244) ist beispielsweise erforderlich, wenn Sie die Bedrohungssignaturen aktualisiert haben und diese bei der Arbeit beschädigt wurden. Sie können zu der vorhergehenden Variante der Signaturen zurückkehren und ihre Aktualisierung später erneut versuchen.

Während die Anwendung aktualisiert wird, können Sie gleichzeitig die Verteilung der heruntergeladenen Updates in eine lokale Quelle ausführen (s. Pkt. 16.4.4 auf S. 254). Dieser Dienst erlaubt es, die Datenbanken und Module, die von Anwendungen der Version 6.0 verwendet werden, auf den Netzwerkcomputern zu aktualisieren und dadurch Netzwerkverkehr einzusparen.

16.1. Starten des Updates

Sie können das Programmupdate jederzeit starten. Die Aktualisierung erfolgt von der von Ihnen gewählten Updatequelle (s. Pkt. 16.4.1 auf S. 246).

Das Programmupdate kann gestartet werden:

- aus dem Kontextmenü (s. Pkt. 4.2 auf S. 53).
- aus dem Hauptfenster des Programms (s. Pkt. 4.3 auf S. 55).

Um das Programmupdate aus dem Kontextmenü zu starten,

1. Öffnen Sie das Menü durch Rechtsklick auf das Programmsymbol im Infobereich.
2. Wählen Sie den Punkt **Update**.

Um das Update aus dem Programmhauptfenster zu starten,

1. Wählen Sie die Komponente **Update** im Abschnitt **Service**.
2. Klicken Sie auf die Schaltfläche **Update** auf der rechten Seite des Hauptfensters oder auf die Schaltfläche in der Statuszeile.

Der Updateprozess des Programms wird in einem speziellen Fenster dargestellt. Sie können das Fenster mit den aktuellen Update-Ergebnissen ausblenden. Klicken Sie dazu auf die Schaltfläche **Schließen**. Der Updatevorgang wird dabei fortgesetzt.

Beachten Sie, dass beim Ausführen des Updates gleichzeitig die Update-Verteilung in eine lokale Quelle erfolgt, falls dieser Dienst aktiviert wurde (s. Pkt. 16.4.4 auf S. 254).

16.2. Rückkehr zum vorherigen Update

Jedes Mal, wenn Sie das Programmupdate starten, erstellt Kaspersky Internet Security zuerst eine Sicherungskopie der aktuellen Bedrohungssignaturen und geht erst danach zu deren Update über. Dadurch wird Ihnen erlaubt, zur Verwendung der vorhergehenden Version der Signaturen zurückzukehren, wenn das Update erfolglos war.

Die Möglichkeit der Rückkehr ist beispielsweise dann nützlich, wenn Sie die Bedrohungssignaturen aktualisiert haben und während der Aktualisierung ein Teil der Signaturen beschädigt wurde, weil die Verbindung unterbrochen wurde.

Sie können zu der vorhergehenden Variante der Signaturen zurückkehren und deren Aktualisierung später erneut versuchen.

Um zur Verwendung der vorhergehenden Version der Bedrohungssignaturen zurückzukehren,

1. Wählen Sie die Komponente **Update** im Abschnitt **Service** des Programmhauptfensters.

2. Klicken Sie auf die Schaltfläche **Rollback** auf der rechten Seite des Hauptfensters.

16.3. Erstellen einer Updateaufgabe

Kaspersky Internet Security verfügt über eine integrierte Updateaufgabe für das Update der Bedrohungssignaturen und Anwendungsmodule. Sie können aber auch eigene Updateaufgaben mit anderen Parametern oder alternativem Startzeitplan erstellen.

Wenn Sie Kaspersky Internet Security beispielsweise auf einem Laptop installiert haben, den Sie zu Hause und im Büro nutzen, kann das Update zu Hause unter Verwendung der Kaspersky-Lab-Server, im Büro aber aus einem lokalen Ordner, der die erforderlichen Updates enthält, erfolgen. Um die Update-Einstellungen nicht jedes Mal ändern zu müssen, können Sie zwei unterschiedliche Aufgaben verwenden.

Um eine zusätzliche Updateaufgabe zu erstellen,

1. Wählen Sie im Abschnitt **Service** des Programmhauptfensters den Punkt **Update**, öffnen Sie mit der rechten Maustaste das Kontextmenü und wählen Sie den Punkt **Speichern unter**.

2. Geben Sie im folgenden Fenster den Namen der Aufgabe an und klicken Sie auf **OK**. Die Aufgabe erscheint mit dem angegebenen Namen im Abschnitt **Service** des Programmhauptfensters.

> Achtung!
>
> Es können maximal Updateaufgaben vom Benutzer erstellt werden.

Die neue Aufgabe übernimmt alle Parameter der Aufgabe, auf deren Grundlage sie erstellt wurde, unter Ausnahme des Zeitplans. Der automatische Start der neuen Aufgabe ist in der Grundeinstellung deaktiviert.

Nehmen Sie nach dem Erstellen einer Aufgabe folgende Zusatzeinstellungen vor: Angabe der Updatequelle und der Parameter für die Netzwerkverbindung. Falls erforderlich, muss außerdem der Aufgabenstart mit Rechten aktiviert und der Zeitplan konfiguriert werden.

Um eine Aufgabe umzubenennen,

wählen Sie die Aufgabe im Abschnitt **Service** des Programmhauptfensters aus, öffnen Sie durch Linksklick das Kontextmenü und wählen Sie den Punkt **Umbenennen**.

Geben Sie im folgenden Fenster den neuen Namen für die Aufgabe an und klicken Sie auf die Schaltfläche **OK**. Dadurch wird der Aufgabenname im Abschnitt **Service** geändert.

Um eine Aufgabe zu löschen,

wählen Sie die Aufgabe im Abschnitt **Service** des Programmhauptfensters aus, öffnen Sie durch Linksklick das Kontextmenü und wählen Sie den Punkt **Löschen**.

Bestätigen Sie das Löschen. Dadurch wird die Aufgabe aus der Aufgabenliste im Abschnitt **Service** gelöscht.

Achtung!

Das Umbenennen und Löschen ist nur für Benutzeraufgaben möglich.

16.4. Update-Einstellungen

Das Programmupdate wird genau nach den Parametern ausgeführt, die festlegen:

- von welcher Ressource der Download und die Installation der Programmupdates erfolgt (s. Pkt. 16.4.1 auf S. 246).
- in welchem Modus der Updateprozess des Programms gestartet wird (s. Pkt. 16.4.2 auf S. 249).
- was aktualisiert werden soll.
- welche Aktionen nach dem Programmupdate ausgeführt werden sollen (s. Pkt. 16.4.4 auf S. 254).

In diesem Abschnitt des Handbuchs werden alle oben genannten Aspekte ausführlich beschrieben.

16.4.1. Auswahl der Updatequelle

Eine *Updatequelle* ist eine bestimmte Ressource, die Updates der Bedrohungssignaturen und der Programm-Module für Kaspersky Internet

Security enthält. Als Updatequelle können http- oder ftp-Server, lokale oder Netzwerkordner dienen.

Als primäre Updatequelle dienen die *Updateserver von Kaspersky Lab*. Das sind spezielle Internetseiten, auf denen die Updates der Bedrohungssignaturen und der Programm-Module für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Wenn Sie keinen Zugriff auf die Kaspersky-Lab-Updateserver besitzen (wenn beispielsweise kein Internetzugang vorhanden ist), können Sie unsere Hauptverwaltung unter der Nummer +7 (495) 797-87-00 anrufen. Dort können Sie die Adressen der Partner von Kaspersky Lab erfahren, die Ihnen die Updates auf Disketten oder CDs im zip-Format anbieten können.

Achtung!

Geben Sie bei der Bestellung von Updates auf Wechseldatenträgern unbedingt an, ob Sie Updates der Programm-Module erhalten möchten.

Die auf einem Wechseldatenträger erhaltenen Updates können Sie auf einer ftp- oder http-Seite oder in einem lokalen oder Netzwerkordner speichern.

Die Auswahl der Updatequelle erfolgt auf der Registerkarte **Updatequelle** (s. Abb. 72).

Die Liste enthält standardmäßig nur die Kaspersky-Lab-Updateserver. Die Serverliste kann nicht verändert werden. Beim Updateprozess greift Kaspersky Internet Security auf diese Liste zu, wählt die erste Serveradresse aus und versucht, die Updates von dort herunterzuladen. Wenn die Aktualisierung von der gewählten Adresse erfolglos ist, wendet sich das Programm an die nächste Adresse und versucht erneut, die Updates zu empfangen. Die Adresse des Servers, von dem das Update erfolgt, wird automatisch an den Listenanfang gerückt. Bei der nächsten Aktualisierung von den Kaspersky-Lab-Updateservern wendet sich das Programm zuerst an den Server, von dem beim vorigen Mal das Update erfolgreich ausgeführt wurde.

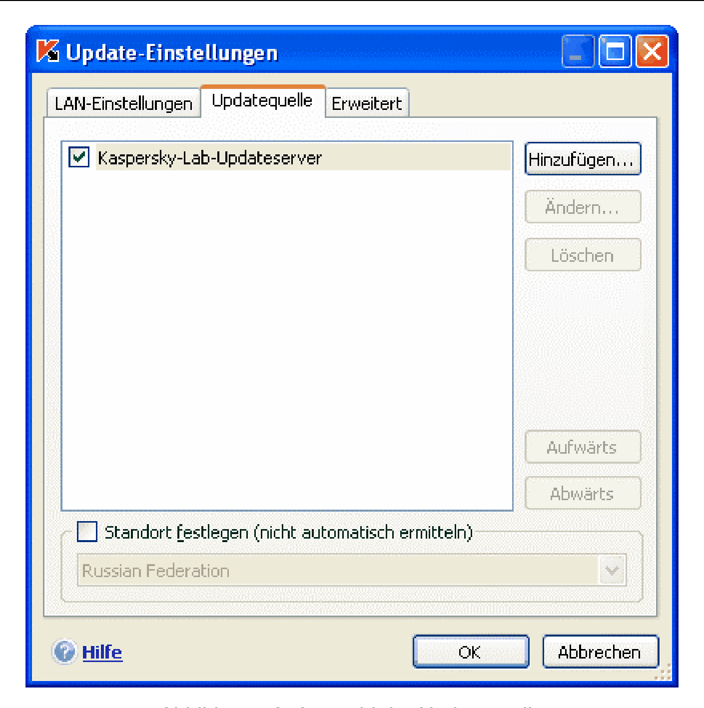


Abbildung 72. Auswahl der Updatequelle

Damit die Aktualisierung von einer bestimmten ftp- oder http-Seite erfolgt,

1. klicken Sie auf die Schaltfläche **Hinzufügen**.
2. wählen Sie die http- oder ftp-Seite im Fenster **Updatequelle wählen** oder geben Sie ihre IP-Adresse, ihren symbolischen Namen oder die URL-Adresse im Feld **Quelle** an.

Achtung!

Wenn Sie als Updatequelle eine Ressource gewählt haben, die sich außerhalb des lokalen Netzwerks befindet, ist für die Aktualisierung eine Internetverbindung erforderlich.

Um das Programm aus einem bestimmten Ordner zu aktualisieren,

1. klicken Sie auf die Schaltfläche **Hinzufügen**.
2. wählen Sie den Ordner im Fenster **Auswahl der Updatequelle** oder geben Sie den vollständigen Pfad des Ordners im Feld **Quelle** an.

Kaspersky Internet Security fügt die neue Updatequelle am Anfang der Liste hinzu und aktiviert sie automatisch zur Verwendung (aktiviert das entsprechende Kontrollkästchen).

Wenn als Updatequellen mehrere Ressourcen gewählt wurden, dann greift das Programm bei der Aktualisierung streng nach der Listenreihenfolge darauf zu und aktualisiert sich von der ersten verfügbaren Quelle. Sie können die Anordnung der Quellen in der Liste mit Hilfe der Schaltflächen **Aufwärts**/**Abwärts** ändern.

Die Quellenliste kann mit den Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** bearbeitet werden. Die Kaspersky-Lab-Updateserver stehen als Quellen nicht für Änderungen oder zum Löschen zur Verfügung.

Wenn Sie die Kaspersky-Lab-Server als Updatequelle verwenden, können Sie den für Sie günstigsten Standort des Servers für den Updatedownload auswählen. Kaspersky Lab besitzt Server in mehreren Ländern der Erde. Die Auswahl des geografisch am nächsten gelegenen Kaspersky-Lab-Updateservers kann die Dauer des Updates verkürzen und die Downloadgeschwindigkeit erhöhen.

Um den nächstliegenden Server zu wählen, aktivieren Sie das Kontrollkästchen ☑ **Standort festlegen (nicht automatisch ermitteln)** und wählen Sie aus der Dropdown-Liste das Land aus, in dem Sie sich gerade aufhalten. Wenn das Kontrollkästchen aktiviert ist, erfolgt das Update unter Berücksichtigung des in der Liste ausgewählten Standorts. Standardmäßig ist das Kontrollkästchen deaktiviert und beim Update werden Informationen über den aktuellen Standort aus der Registrierung des Betriebssystems verwendet.

Beachten Sie, dass die Option zur Auswahl des Updateservers, der geografisch am nächsten liegt, im Programm nicht verfügbar ist, wenn es auf einem Computer mit Microsoft Windows 9x/NT 4.0 installiert wird.

16.4.2. Auswahl von Updatemodus und Update-Objekt

Ein wichtiger Faktor bei der Konfiguration des Programmupdates ist das Festlegen von Update-Objekt und Updatemodus.

Das Update-Objekt (s. Abb. 73) bestimmt, welche Elemente aktualisiert werden:

- Bedrohungssignaturen
- Netzwerktreiber, die die Funktionalität für das Abfangen des Netzwerkverkehrs durch die Schutzkomponenten gewährleisten.

- Datenbank der Netzwerkangriffe, die bei der Arbeit von Anti-Hacker verwendet werden.
- Programm-Module

Bedrohungssignaturen, Netzwerktreiber und Angriffssignaturen werden immer aktualisiert, die Programm-Module nur dann, wenn der entsprechende Modus aktiviert ist.



Abbildung 73. Auswahl des Update-Objekts

Damit beim Updateprozess die Updates der Programm-Module auf Ihren Computer kopiert und installiert werden,

aktivieren Sie das Kontrollkästchen ☑ **Programm-Module aktualisieren** im Konfigurationsfenster der Komponente **Update**.

Wenn im Augenblick der Aktualisierung an der Quelle ein Update der Programm-Module vorhanden ist, wird ein spezielles Fenster auf dem Bildschirm angezeigt, das eine Beschreibung aller aktuellen Änderungen der Programm-Module enthält. Aufgrund dieser Beschreibung können Sie entscheiden, ob das Update installiert werden soll oder nicht.

Der Updatemodus (s. Abb. 74) bestimmt, auf welche Weise die Aktualisierung gestartet wird. Sie können einen der folgenden Modi wählen:

◉ **Automatisch**. Kaspersky Internet Security prüft in festgelegten Zeitabständen, ob an der Updatequelle (s. Pkt. 16.4.1 auf S. 246) ein neues Updatepaket vorhanden ist. Wenn neue Updates vorliegen, lädt Kaspersky Internet Security sie herunter und installiert sie auf dem Computer. Dieser Updatemodus wird standardmäßig benutzt.

Wenn als Quelle eine Netzwerkressource gewählt wurde, führt Kaspersky Internet Security in dem Intervall, das im vorhergehenden Updatepaket angegeben ist, einen Updateversuch durch. Aus einer lokalen Quelle erfolgt das Update im Intervall, das im vorhergehenden Updatepaket angeben ist. Diese Option erlaubt es, die Updatefrequenz bei Virenepidemien und anderen gefährlichen Situationen automatisch zu regulieren. Das Programm wird rechtzeitig mit aktuellen Updates der Bedrohungssignaturen, Netzwerkangriffe und Programm-Module versorgt, was die Möglichkeit des Eindringens gefährlicher Programme auf Ihren Computer verhindert.



Abbildung 74. Auswahl des Startmodus für das Update

- **Nach Zeitplan**. Die Aktualisierung des Programms erfolgt nach einem festgelegten Zeitplan. Wenn Sie zu diesem Updatemodus wechseln möchten, wird Ihnen standardmäßig angeboten, das Update einmal täglich vorzunehmen. Um den Zeitplan anzupassen, klicken Sie auf die Schaltfläche **Ändern** neben der Bezeichnung des Modus und nehmen Sie im folgenden Fenster entsprechende Änderungen vor (Details s. Pkt. 6.5 auf S. 91).
- **Manuell**. In diesem Fall starten Sie die Aktualisierung des Programms selbständig. Kaspersky Internet Security informiert Sie bei Bedarf über die Notwendigkeit der Aktualisierung:
  - erstens wird über dem Programmsymbol im Infobereich eine entsprechende Meldung eingeblendet (wenn der Benachrichtigungsdienst aktiviert ist) (s. Pkt. 17.11.1 auf S. 299).
  - zweitens informiert der zweite Indikator im Programmhauptfenster darüber, wenn der Schutz auf ihrem Computer veraltet ist (s. Pkt. 5.1.1 auf S. 61).
  - drittens erscheint im Bereich der Kommentare und Empfehlungen des Hauptfensters eine Empfehlung zum Programmupdate (s. Pkt. 4.3 auf S. 55).

16.4.3. Konfiguration der Verbindungsparameter

Wenn Sie als Updatequelle die Kaspersky-Lab-Updateserver oder eine bestimmte ftp- oder http-Seite gewählt haben, ist es empfehlenswert, die Einstellungen für die Internetverbindung zu überprüfen.

Standardmäßig werden für die Internetverbindung die Parameter verwendet, die Alle Parameter sind auf der speziellen Registerkarte **LAN-Einstellungen** untergebracht (s. Abb. 75).

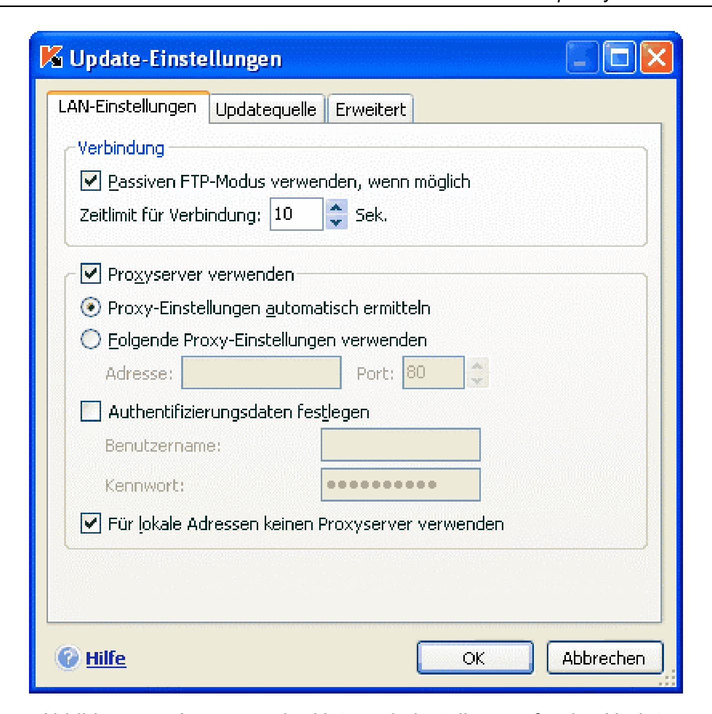


Abbildung 75. Anpassen der Netzwerkeinstellungen für das Update

Der Parameter **Passiven FTP-Modus verwenden, wenn möglich** wird verwendet, wenn Sie Updates von einem ftp-Server herunterladen, mit dem eine Verbindung im passiven Modus ausgeführt wird (beispielsweise über eine Firewall). Wenn der aktive Modus für die FTP-Verbindung benutzt wird, können Sie dieses Kontrollkästchen deaktivieren.

Geben Sie im Feld **Zeitlimit für Verbindung (Sek.)** den Zeitraum an, der zur Verfügung stehen soll, um eine Verbindung mit dem Updateserver aufzubauen. Wenn nach Ablauf dieses Zeitraums keine Verbindung hergestellt wurde, erfolgt ein Verbindungsversuch mit dem nächsten Updateserver. Dieser Vorgang wird so lange ausgeführt, bis der Verbindungsaufbau gelingt oder bis alle verfügbaren Updateserver aufgerufen worden sind.

Wenn für die Internetverbindung ein Proxyserver verwendet wird, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und passen Sie bei Bedarf folgende Parameter an:

- Wählen Sie, welche Proxyserver-Einstellungen für das Programmupdate verwendet werden sollen:

- **Proxy-Einstellungen automatisch ermitteln**. Bei Auswahl dieser Variante werden die Parameter des Proxyservers automatisch mit Hilfe des Protokolls WPAD (Web Proxy Auto-Discovery Protocol) ermittelt. Falls die Adresse mit diesem Protokoll nicht ermittelt werden kann, verwendet Kaspersky Internet Security die Proxy-Einstellungen, die in Microsoft Internet Explorer angegeben sind.
- **Folgende Proxy-Einstellungen verwenden** – Einen anderen Proxyserver verwenden, als jenen, der in den Verbindungseinstellungen des Browsers angegeben ist. Geben Sie im Feld **Adresse** die IP-Adresse oder den symbolischen Namen und im Feld **Port** den Port des Proxyservers an, der für das Programmupdate benutzt werden soll.

- Geben Sie an, ob auf dem Proxy eine Authentifizierung verwendet wird. Die *Authentifizierung* ist ein Vorgang, bei dem zum Zweck der Zugriffskontrolle die Anmeldungsdaten des Benutzers geprüft werden.

  Wenn für eine Verbindung mit dem Proxyserver die Authentifizierung erforderlich ist, aktivieren Sie das Kontrollkästchen **Authentifizierungsdaten festlegen** und geben Sie in den unten angebrachten Feldern den Benutzernamen und das Kennwort an. In diesem Fall wird zuerst die NTLM-Autorisierung, danach die BASIC-Autorisierung versucht.

  Wenn das Kontrollkästchen nicht aktiviert ist oder keine Daten angegeben werden, wird die NTLM-Autorisierung versucht, wobei das Benutzerkonto verwendet wird, in dessen Namen das Update gestartet wurde ist (s. Pkt. 6.4 auf S. 89).

  Wenn die Autorisierung auf dem Proxyserver erforderlich ist, Sie aber den Benutzernamen und das Kennwort nicht angegeben haben oder der Proxyserver die angegebenen Daten aus einem beliebigen Grund nicht akzeptiert, erscheint beim Updatestart eine Anfrage nach Benutzername und Kennwort für die Autorisierung. Wenn die Autorisierung erfolgreich verläuft, werden der angegebene Benutzername und das Kennwort auch beim nächsten Update verwendet. Andernfalls werden die Autorisierungsparameter erneut abgefragt.

Damit beim Update aus einem lokalen Ordner oder Netzwerkordner kein Proxyserver verwendet wird, aktivieren Sie das Kontrollkästchen **Für lokale Adressen keinen Proxyserver verwenden**.

> Dieser Parameter steht nicht zur Verfügung, wenn das Programm auf einem Computer mit Microsoft Windows 9X/NT 4.0 installiert ist. Allerdings wird für lokale Adressen standardmäßig kein Proxyserver verwendet.

16.4.4. Update-Verteilung

Wenn PCs zu einem lokalen Netzwerk zusammengeschlossen sind, ist es überflüssig die Updates für jeden Computer einzeln herunterzuladen und zu installieren, weil dadurch eine erhöhte Netzwerkbelastung verursacht wird. Sie können den Dienst zur Update-Verteilung verwenden, der es erlaubt, die Netzwerkbelastung zu senken, indem das Updateverfahren folgendermaßen organisiert wird:

1. Ein Computer des Netzwerks lädt das Paket mit den Updates für Anwendungsmodule und Bedrohungssignaturen von den Kaspersky-Lab-Webservern im Internet oder von einer anderen Webressource, auf der sich die aktuellen Updates befinden, herunter. Die heruntergeladenen Updates werden in einem gemeinsamen Ordner abgelegt.

2. Die übrigen Netzwerkcomputer verwenden den gemeinsamen Ordner zum Download der Updates für die Anwendung.

Um den Dienst zur Update-Verteilung zu aktivieren, kreuzen Sie auf der Registerkarte **Erweitert** (s. Abbildung 76) das Kontrollkästchen ☑ **Zielordner für Update-Verteilung** an und geben Sie im darunter liegenden Feld den Pfad des gemeinsamen Ordners an, in dem die heruntergeladenen Updates abgelegt werden. Der Pfad kann manuell eingegeben oder im Fenster, das mit der Schaltfläche **Durchsuchen** geöffnet wird, gewählt werden. Wenn das Kontrollkästchen aktiviert ist, werden neue Updates beim Download automatisch in diesen Ordner kopiert.

Zusätzlich können Sie die Methode für die Update-Verteilung festlegen:

- *vollständige Verteilung* – In diesem Fall werden die Bedrohungssignaturen und Updates der Komponenten für alle Kaspersky-Lab-Anwendungen der Version 6.0 kopiert. Um das vollständige Update zu wählen, aktivieren Sie das Kontrollkästchen ☑ **Updates für alle Komponenten kopieren**.

- *Verteilung ausgewählter Elemente* – Dabei werden die Bedrohungssignaturen sowie Updates nur für die installierten Komponenten von Kaspersky Internet Security 6.0 kopiert. Um diese Updatemethode zu wählen, muss das Kontrollkästchen ☑ **Updates für alle Komponenten kopieren** deaktiviert werden.

Beachten Sie, dass Kaspersky Internet Security 6.0 von den Kaspersky-Lab-Updateservern nur das Updatepaket für die Anwendungen der Version 6.0 erhält.

Damit die anderen Netzwerkcomputer aus dem Ordner aktualisiert werden, der die aus dem Internet kopierten Updates enthält, sind folgende Einstellungen erforderlich.

1. Der gemeinsame Zugriff auf diesen Ordner muss gewährt werden.
2. Der gemeinsame Ordner muss in den Update-Einstellungen der Netzwerkcomputer als Updatequelle angegeben werden.

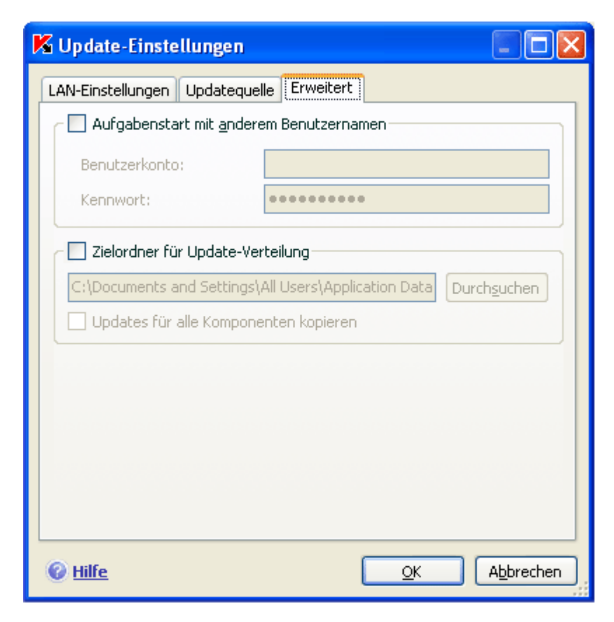


Abbildung 76. Einstellungen für den Dienst zur Update-Verteilung

16.4.5. Aktionen nach dem Programmupdate

Jedes Update der Bedrohungssignaturen enthält neue Einträge, die es erlauben, Ihren Computer vor neu aufgetauchten Bedrohungen zu schützen.

Die Kaspersky-Lab-Spezialisten empfehlen Ihnen, sofort nach dem Programmupdate die *in der Quarantäne gespeicherten Objekte* und die *Autostart-Objekte* zu untersuchen.

Warum gerade diese Objekte?

In die Quarantäne werden Objekte verschoben, bei deren Untersuchung nicht genau festgestellt werden konnte, von welchen schädlichen Programmen sie infiziert sind (s. Pkt. 17.1 auf S. 258). Möglicherweise kann Kaspersky Internet Security die Gefahr eindeutig bestimmen und desinfizieren, nachdem die Bedrohungssignaturen aktualisiert wurden.

Das Programm untersucht die Quarantäneobjekte standardmäßig nach jedem Update der Bedrohungssignaturen. Es wird empfohlen, die Objekte in der Quarantäne regelmäßig zu überprüfen. Aufgrund der Untersuchung kann sich der Status einzelner Objekte ändern. Bestimmte Objekte können am ursprünglichen Ort wiederhergestellt und wieder verwendet werden.

Damit keine Untersuchung der Quarantäneobjekte erfolgt, deaktivieren Sie das Kontrollkästchen ☑ **Quarantänedateien untersuchen** im Block **Aktion nach dem Update**.

Die Autostart-Objekte gelten hinsichtlich der Sicherheit Ihres Computers als kritischer Bereich. Wenn dieser Bereich von einem Schadprogramm infiziert wird, ist vielleicht sogar der Start des Betriebssystems nicht mehr möglich. Zur Untersuchung dieses Bereichs verfügt Kaspersky Internet Security über eine vordefinierte Aufgabe zur Untersuchung der Autostart-Objekte (s. Kapitel 14 auf S. 221). Es wird empfohlen, den Zeitplan dieser Aufgabe so festzulegen, dass sie jedes Mal nach dem Update der Bedrohungssignaturen automatisch gestartet wird (s. Pkt. 6.5 auf S. 91).

KAPITEL 17. ZUSÄTZLICHE OPTIONEN

Neben dem Schutz Ihrer Daten bietet das Programm zusätzliche Dienste, welche die Funktionalität von Kaspersky Internet Security erweitern.

Während der Arbeit verschiebt das Programm bestimmte Objekte in spezielle Speicher. Das Ziel dieses Vorgehens besteht darin, maximalen Datenschutz mit minimalen Verlusten zu gewährleisten.

- Der Backup-Speicher enthält Kopien der Objekte, die aufgrund der Arbeit von Kaspersky Internet Security verändert oder gelöscht wurden (s. Pkt. 17.2 auf S. 262). Wenn ein bestimmtes Objekt wichtige Informationen enthielt, die bei der Bearbeitung nicht vollständig erhalten werden konnten, können Sie das Objekt jederzeit über seine Sicherungskopie wiederherstellen.
- Die Quarantäne enthält möglicherweise infizierte Objekte, deren Desinfektion mit der aktuellen Version der Bedrohungssignaturen erfolglos war (s. Pkt. 17.1 auf S. 258).

Es wird empfohlen, die Liste der Objekte immer wieder zu überprüfen. Möglicherweise befinden sich veraltete Objekte darunter oder bestimmte Objekte können wiederhergestellt werden.

Folgende Dienste helfen bei der Arbeit mit dem Programm:

- Der Dienst des Technischen Support-Service bietet umfassende Hilfe bei der Arbeit mit Kaspersky Internet Security (s. Pkt. 17.5 auf S. 283). Die Experten von Kaspersky Lab haben sich bemüht, alle vorhandenen Unterstützungsmöglichkeiten zu integrieren: Online-Support, Forum für Fragen und Vorschläge der Programmbenutzer usw.
- Der Benachrichtigungsdienst für Ereignisse hilft Ihnen bei der Konfiguration einer Benachrichtigung des Benutzers über wichtige Momente bei der Arbeit von Kaspersky Internet Security (s. Pkt. 17.11.1 auf S. 299). Dies können einerseits Ereignisse informativen Charakters sein, andererseits aber Fehler, die unverzüglich behoben werden müssen und hohe Priorität besitzen.
- Der Dienst für den Selbstschutz des Programms und für die Beschränkung des Zugriffs auf die Arbeit mit dem Programm bietet den programmeigenen Dateien Schutz vor Veränderungen und Beschädigungen durch Angreifer, verbietet die externe Steuerung der Programmdienste und kontrolliert die Beschränkung von Rechten anderer

Benutzer Ihres Computers zum Ausführen bestimmter Aktionen mit Kaspersky Internet Security (s. Pkt. 17.11.1.3 auf S. 303). Beispielsweise kann das Ändern der Schutzstufe wesentlichen Einfluss auf die Informationssicherheit auf Ihrem Computer ausüben.

- Der Dienst zur Verwaltung von Lizenzschlüsseln erlaubt es, ausführliche Informationen über die verwendete Lizenz zu erhalten, Ihre Programmkopie zu aktivieren sowie Lizenzschlüsseldateien zu verwalten (s. Pkt. 17.5 auf S. 283).

Darüber hinaus bietet das Programm ein ausführliches Hilfesystem (s. Pkt. 17.4 auf S. 282) und detaillierte Berichte (s. Pkt. 17.3 auf S. 265) über die Arbeit aller Schutzkomponenten und die Ausführung aller Aufgaben zur Virensuche.

Das Erstellen einer Port-Liste erlaubt es, die Kontrolle der durch die Schutzkomponenten von Kaspersky Internet Security über die Ports empfangenen und weitergeleiteten Informationen zu regulieren (s. Pkt. 17.7 auf S. 287).

Die Option für das Erstellen einer Notfall-CD zur Systemwiederherstellung erlaubt es, die Funktionsfähigkeit des Computers in dem Zustand wiederherzustellen, der vor einer Infektion herrschte (s. Pkt. 17.10 auf S. 294). Das kann besonders nützlich sein, wenn Systemdateien durch schädlichen Code beschädigt wurden und das Betriebssystem des Computers nicht mehr geladen werden kann.

Außerdem besteht die Möglichkeit, das Aussehen von Kaspersky Internet Security zu ändern und die Parameter der aktuellen Programmoberfläche zu konfigurieren (s. Pkt. 17.8 auf S. 290).

Im Folgenden werden alle genannten Dienste ausführlich beschrieben.

17.1. Quarantäne für möglicherweise infizierte Objekte

Die **Quarantäne** ist ein spezieller Speicher, in den Objekte verschoben werden, die möglicherweise von Viren infiziert sind.

Möglicherweise infizierte Objekte sind Objekte, die verdächtig sind, von Viren oder Virenmodifikationen infiziert zu sein.

Warum *möglicherweise infiziert*? Es ist nicht immer möglich, eindeutig festzustellen, ob ein Objekt infiziert ist oder nicht. Dafür gibt es folgende Gründe:

- *Der Code des analysierten Objekts besitzt Ähnlichkeit mit einer bekannten Bedrohung, wurde aber teilweise verändert*.

  Die Bedrohungssignaturen enthalten jene Bedrohungen, die bisher von den Kaspersky-Lab-Spezialisten untersucht wurden. Wenn ein Schadprogramm verändert wird und diese Veränderungen noch nicht in die Signaturen aufgenommen wurden, klassifiziert Kaspersky Internet Security das Objekt, das von einem veränderten Schadprogramm infiziert ist, als möglicherweise infiziertes Objekt und informiert darüber, welcher Bedrohung diese Infektion ähnelt.

- *Der Code des gefundenen Objekts erinnert an die Struktur eines Schadprogramms. Die Bedrohungssignaturen enthalten jedoch keine entsprechenden Einträge.*

  Es ist durchaus möglich, dass es sich um eine neue Art von Bedrohung handelt. Deshalb klassifiziert Kaspersky Internet Security dieses Objekt als möglicherweise infiziertes Objekt.

Der Verdacht, dass eine Datei durch einen Virus infiziert ist, wird mit dem *heuristischen Code Analysator* ermittelt, mit dessen Hilfe bis zu 92 % aller neuen Viren erkannt werden. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Ein verdächtiges Objekt kann während der Virensuche sowie bei der Arbeit von Datei-Anti-Virus, Mail-Anti-Virus und Proaktivem Schutz gefunden und in die Quarantäne verschoben werden.

Sie können eine Datei selbst in die Quarantäne verschieben. Dazu dient die Schaltfläche **Quarantäne** in der speziellen Meldung, die beim Fund eines möglicherweise infizierten Objekts auf dem Bildschirm Ihres Computers erscheint.

Beim Speichern eines Objekts in die Quarantäne wird das Objekt verschoben, nicht kopiert: Das Objekt wird von dem entsprechenden Laufwerk oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

17.1.1. Aktionen mit Objekten in der Quarantäne

Die Gesamtzahl der Objekte, die in die Quarantäne verschoben wurden, wird im Bereich **Datenverwaltung** des Abschnitts **Service** angezeigt. Auf der rechten Seite des Hauptfensters befindet sich der spezielle Block **Quarantäne**, der folgende Daten enthält:

- Anzahl der möglicherweise infizierten Objekte, die während der Arbeit von Kaspersky Internet Security gefunden wurden.
- aktuelle Größe des Speichers.

Mit der Schaltfläche **Leeren** können alle Quarantäneobjekte gelöscht werden. Beachten Sie, dass dabei auch die Objekte des Backups und die Berichtsdateien gelöscht werden.

Um zu den Quarantäneobjekten zu wechseln,

klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Quarantäne**.

Auf der Registerkarte **Quarantäne** (s. Abb. 77) können Sie folgende Aktionen vornehmen:

- Verschieben einer Datei in die Quarantäne, wenn Sie vermuten, dass die Datei von einem Virus infiziert ist, den das Programm nicht finden konnte. Klicken Sie dazu auf die Schaltfläche **Hinzufügen** und geben Sie im standardmäßigen Auswahlfenster die betreffende Datei an. Sie wird mit dem Status *Vom Benutzer hinzugefügt* zur Liste hinzugefügt.

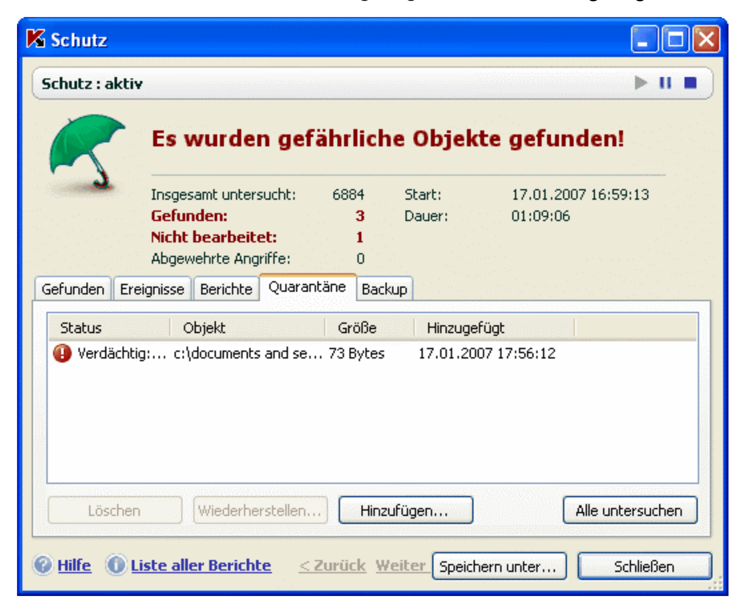


Abbildung 77. Liste der Quarantäneobjekte

- Alle möglicherweise infizierten Quarantäneobjekte unter Verwendung der aktuellen Version der Bedrohungssignaturen untersuchen und desinfizieren. Klicken Sie dazu auf die Schaltfläche **Alle untersuchen**.

  Aufgrund der Untersuchung und Desinfektion eines beliebigen Quarantäne-Objekts kann sich sein Status in *infiziert*, *möglicherweise infiziert*, *Fehlalarm*, *ok* u.a. ändern.

  Der Objektstatus *infiziert* bedeutet, dass das Objekt als infiziert erkannt wurde, die Desinfektion aber fehlgeschlagen ist. Wir empfehlen, Objekte mit diesem Status zu löschen.

  Alle Objekte mit dem Status *Fehlalarm* können bedenkenlos wiederhergestellt werden, weil ihr vorheriger Status *möglicherweise infiziert* bei einer erneuten Untersuchung vom Programm nicht bestätigt wurde.

- Dateien wiederherstellen – entweder in einem vom Benutzer gewählten Ordner oder in den Ordnern, aus denen sie (standardmäßig) in die Quarantäne verschoben wurden. Zum Wiederherstellen eines Objekts markieren Sie es in der Liste und klicken Sie auf **Wiederherstellen**. Bei der Wiederherstellung von Objekten, die aus Archiven, Maildatenbanken und Mail-Format-Dateien in die Quarantäne verschoben wurden, muss zusätzlich der Ordner angegeben werden, in dem sie wiederhergestellt werden sollen.

  > Empfehlung:
  >
  > Es wird empfohlen, nur Objekte mit dem Status *Fehlalarm*, *ok* und *desinfiziert* wiederherzustellen, da die Wiederherstellung anderer Objekte zur Infektion Ihres Computers führen kann!

- Ein beliebiges Quarantäne-Objekt oder eine Gruppe ausgewählter Objekte löschen. Löschen Sie nur die Objekte, die nicht desinfiziert werden können. Klicken Sie auf die Schaltfläche **Löschen**, um Objekte zu löschen.

17.1.2. Konfiguration der Quarantäne-Einstellungen

Sie können folgende Parameter für das Erstellen und die Arbeit der Quarantäne anpassen:

- Auswahl des Modus zur automatischen Untersuchung von Objekten in der Quarantäne nach jedem Update der Bedrohungssignaturen (Details s. Pkt. 16.4.4 auf S. 254).

> Achtung!
>
> Das Programm kann die Quarantäneobjekte nicht unmittelbar nach der Aktualisierung der Bedrohungssignaturen untersuchen, wenn Sie in diesem Moment mit der Quarantäne arbeiten.

- Festlegen der maximalen Speicherdauer für Objekte in der Quarantäne.

  Standardmäßig beträgt die Speicherdauer für Quarantäneobjekte 30 Tage. Danach werden die Objekte gelöscht. Sie können die maximale Speicherdauer für möglicherweise infizierte Objekte ändern oder diese Beschränkung ganz aufheben.

Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security mit der Schaltfläche Einstellungen aus dem Programmhauptfenster.
2. Wählen Sie **Datenverwaltung** in der Konfigurationsstruktur.
3. Legen Sie im Block **Quarantäne und Backup** (s. Abb. 78) den Zeitraum fest, nach dem Quarantäneobjekte automatisch gelöscht werden sollen.



Abbildung 78. Anpassen der Speicherdauer für Quarantäneobjekte

17.2. Sicherungskopien gefährlicher Objekte

Bei der Desinfektion von Objekten kann es vorkommen, dass es nicht gelingt, die Objekte vollständig zu erhalten. Wenn ein desinfiziertes Objekt wichtige Informationen enthielt, die aufgrund der Desinfektion vollständig oder teilweise verloren gingen, kann versucht werden, das ursprüngliche Objekt über seine Sicherungskopie wiederherzustellen.

Eine **Sicherungskopie** ist die Kopie eines gefährlichen Originalobjekts, die bei der ersten Desinfektion oder beim Löschen des Objekts erstellt und im Backup gespeichert wird.

Der **Backup-Speicher** ist ein spezieller Speicher, der die Sicherungskopien gefährlicher Objekte enthält, die bearbeitet oder gelöscht werden. Die Hauptfunktion des Backups besteht in der Möglichkeit, das ursprüngliche Objekt

jederzeit wiederherzustellen. Die Sicherungskopien werden im Backup in einem speziellen Format gespeichert und stellen keine Gefahr dar.

17.2.1. Aktionen mit Sicherungskopien

Die Gesamtzahl der Sicherungskopien von Objekten, die sich im Backup befinden, wird in der **Datenverwaltung** des Abschnitts **Service** genannt. Auf der rechten Seite des Hauptfensters befindet sich der spezielle Block **Backup**, der folgende Daten enthält:

- Anzahl der Kopien von möglicherweise infizierten Objekten, die während der Arbeit von Kaspersky Internet Security angelegt wurden.
- aktuelle Größe des Backup-Speichers.

Mit der Schaltfläche **Leeren** können alle Sicherungskopien aus dem Backup gelöscht werden. Beachten Sie, dass dabei auch die Objekte aus der Quarantäne und die Berichtsdateien gelöscht werden.

Um zu den Kopien der gefährlichen Objekte zu wechseln,

klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Backup**.

Im mittleren Bereich der Registerkarte **Backup** (s. Abb. 79) befindet sich eine Liste der Sicherungskopien. Für jede Kopie werden folgende Informationen angegeben: vollständiger Name des Objekts mit dem Pfad des ursprünglichen Speicherorts, Status des Objekts, der ihm aufgrund der Untersuchung zugewiesen wurde, und Größe.

Sie können ausgewählte Kopien mit Hilfe der Schaltfläche **Wiederherstellen** wiederherstellen. Das Objekt wird unter dem gleichen Namen aus dem Backup wiederhergestellt, den es vor der Desinfektion trug.

Wenn sich am ursprünglichen Speicherort ein Objekt mit dem gleichen Namen befindet (Diese Situation ist möglich, wenn ein Objekt wiederhergestellt wird, dessen Kopie vor der Desinfektion angelegt wurde), erscheint eine entsprechende Warnung auf dem Bildschirm. Sie können den Speicherort des wiederherzustellenden Objekts ändern oder es umbenennen.

Es wird empfohlen, das Objekt sofort nach der Wiederherstellung auf Viren zu untersuchen. Möglicherweise gelingt es, das Objekt mit den aktualisierten Signaturen ohne Datenverlust zu desinfizieren.

Es wird davor gewarnt, Sicherungskopien von Objekten wiederherzustellen, wenn es nicht absolut erforderlich ist. Dies kann zur Infektion des Computers führen.

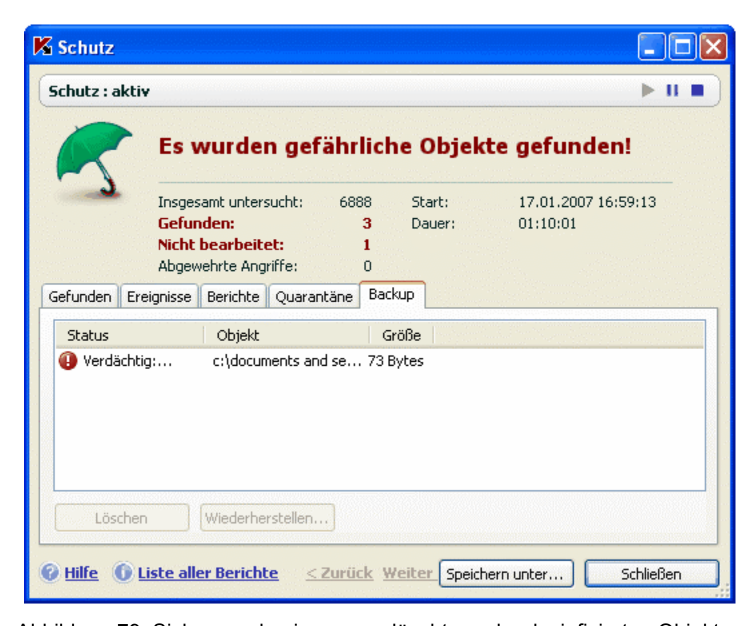


Abbildung 79. Sicherungskopien von gelöschten oder desinfizierten Objekten

Es wird empfohlen, den Speicher in bestimmten Zeitabständen zu überprüfen und überflüssige Objekte mit Hilfe der Schaltfläche **Löschen** zu entfernen. Sie können das Programm auch so konfigurieren, dass es selbständig die ältesten Kopien aus dem Speicher löscht (s. Pkt. 17.2.2 auf S. 264).

17.2.2. Konfiguration der Backup-Einstellungen

Sie können die maximale Speicherdauer der Kopien im Backup festlegen.

Standardmäßig beträgt die Speicherdauer für Kopien gefährlicher Objekte 30 Tage. Danach werden die Kopien gelöscht. Sie können die maximale Speicherdauer für Kopien ändern oder diese Beschränkung ganz aufheben. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security mit der Schaltfläche Einstellungen aus dem Programmhauptfenster.
2. Wählen Sie **Datenverwaltung** in der Konfigurationsstruktur.

3. Legen Sie die Speicherdauer für Sicherungskopien im Block **Quarantäne und Backup** auf der rechten Seite des Fensters fest (s. Abb. 78).

17.3. Berichte

Die Arbeit jeder Komponente von Kaspersky Internet Security und die Ausführung jeder Aufgabe zur Virensuche und des Updates werden in einem Bericht aufgezeichnet.

Über die Gesamtzahl der Berichte, die bisher vom Programm erstellt wurden, sowie ihre Gesamtgröße in Bytes wird in der **Datenverwaltung** des Abschnitts **Service** des Programmhauptfensters informiert. Diese Informationen befinden sich im Block **Berichte**.

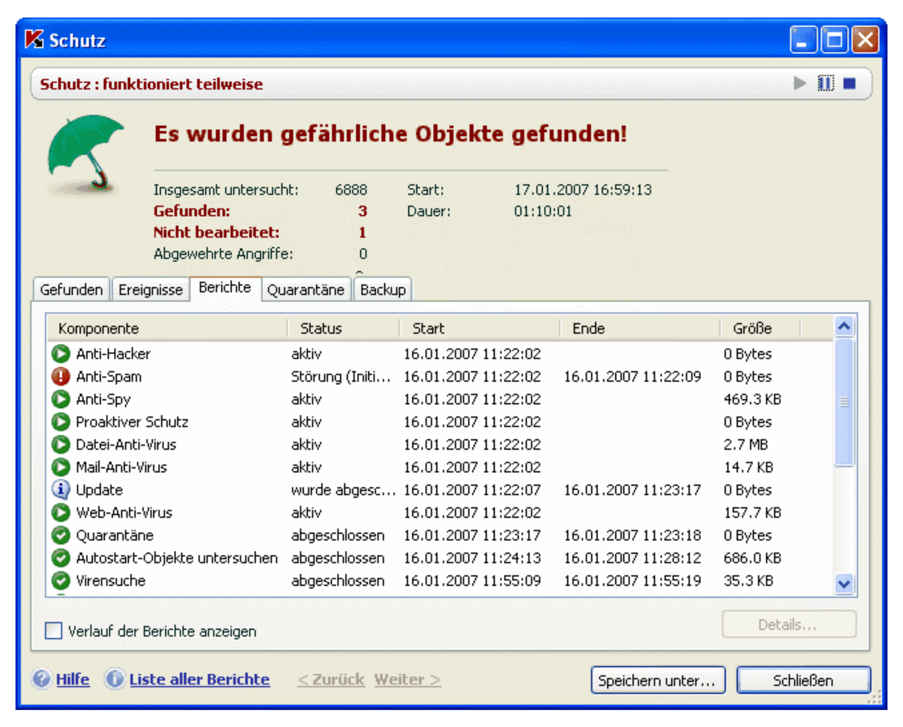


Abbildung 80. Berichte über die Arbeit der Programmkomponenten

Um zur Anzeige der Berichte zu wechseln,

klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Berichte**.

Dadurch wird das Fenster auf der Registerkarte **Berichte** geöffnet (s. Abb. 80). Hier befinden sich die neuesten Berichte für alle Komponenten und Aufgaben zur Virensuche, die in der laufenden Sitzung von Kaspersky Internet Security gestartet wurden. Neben jeder Komponente und Aufgabe wird das Arbeitsergebnis genannt (beispielsweise *abgebrochen* oder *abgeschlossen*). Wenn Sie den vollständigen Verlauf der Berichtserstellung für die laufende Programmsitzung lesen möchten, aktivieren Sie das Kontrollkästchen ☑ **Verlauf der Berichte anzeigen**.

Um alle Ereignisse anzuzeigen, die im Bericht über die Arbeit einer Komponente oder die Ausführung einer Aufgabe aufgezeichnet wurden,

wählen Sie den Namen der Komponente oder Aufgabe auf der Registerkarte **Berichte** und klicken Sie auf die Schaltfläche **Details**.

Dadurch wird ein Fenster geöffnet, das Detailinformationen über die Arbeit der gewählten Komponente oder Aufgabe enthält. Die Ergebnisstatistik der Arbeit befindet sich im oberen Bereich des Fensters, ausführliche Informationen befinden sich auf verschiedenen Registerkarten im mittleren Bereich. Abhängig von der Komponente oder Aufgabe unterscheidet sich der Aufbau der Registerkarten:

- Die Registerkarte **Gefunden** enthält eine Liste der gefährlichen Objekte, die bei der Arbeit der Komponente oder beim Ausführen einer Untersuchungsaufgabe gefunden wurden.
- Die Registerkarte **Ereignisse** informiert über die Ereignisse bei der Arbeit einer Komponente oder Aufgabe.
- Die Registerkarte **Statistik** umfasst eine ausführliche Statistik aller untersuchten Objekte.
- Die Registerkarte **Einstellungen** enthält die Parameter, mit denen die Schutzkomponente, Aufgabe zur Virensuche oder das Update der Bedrohungssignaturen arbeitet.
- Die Registerkarten **Makros** und **Registrierung** sind nur im Bericht des Proaktiven Schutzes vorhanden und enthalten Informationen über alle Makros, die auf Ihrem Computer gestartet werden sollten, sowie über alle Versuche zum Ändern der Systemregistrierung des Betriebssystems.
- Die Registerkarten **Phishing-Seiten**, **Popup-Fenster**, **Banner** und **Versuche zur Auto-Einwahl** sind nur im Bericht von Anti-Spy vorhanden. Sie enthalten Informationen über alle erkannten Versuche zu Phishing-Angriffen, über alle während der laufenden Programmsitzung blockierten

Popup-Fenster, Banner und Versuche zur automatischen Einwahl auf kostenpflichtige Internetressourcen.

- Die Registerkarten **Netzwerkangriffe**, **Blockierte Hosts**, **Anwendungsaktivität** und **Paketfilterung** sind nur im Bericht von Anti-Hacker vorhanden. Sie enthalten Informationen über alle auf Ihren Computer versuchten Netzwerkangriffe und die aufgrund der Angriffsversuche blockierten Hosts. Außerdem informieren sie über die Netzwerkaktivität der Anwendungen, die unter die vorhandenen Aktivitätsregeln fallen, sowie über alle Datenpakete, für welche die Regeln zur Paketfilterung von Anti-Hacker gelten.
- Die Registerkarten **Aktive Verbindungen**, **Offene Ports** und **Datenverkehr** charakterisieren ebenfalls die Netzwerkaktivität auf Ihrem Computer. Sie informieren über bestehende Verbindungen, geöffnete Ports und über das Volumen des von Ihrem Computer gesendeten und empfangenen Datenverkehrs.

Sie können den gesamten Bericht in eine Textdatei importieren. Das kann beispielsweise von Nutzen sein, wenn bei der Arbeit einer Komponente oder bei der Aufgabenausführung ein Fehler aufgetreten ist, den Sie nicht selbständig beseitigen können, und deshalb die Hilfe des technischen Support-Service erforderlich ist. In diesem Fall wird der Bericht im Textformat an den Support-Service geschickt, damit unsere Spezialisten das Problem genau untersuchen und so schnell wie möglich lösen können.

Um einen Bericht in eine Textdatei zu importieren,

klicken Sie auf die Schaltfläche **Speichern unter** und geben Sie an, wo die Berichtsdatei gespeichert werden soll.

Klicken Sie zum Abschluss der Arbeit mit dem Bericht auf die Schaltfläche **Schließen**.

Alle Registerkarten des Berichts außer **Einstellungen** und **Statistik** verfügen über die Schaltfläche **Aktionen**, mit deren Hilfe Sie eine Reihe von Aktionen mit den Objekten der Liste vornehmen können. Durch Klick auf diese Schaltfläche öffnet sich ein Kontextmenü mit folgenden Punkten (Die Auswahl der Menüpunkte unterscheidet sich in Abhängigkeit von der Komponente, deren Bericht Sie geöffnet haben. Unten werden alle möglichen Punkte genannt):

- **Desinfizieren** – Es wird versucht, das gefährliche Objekt zu desinfizieren. Wenn die Desinfektion des Objekts fehlschlägt, können Sie es entweder in der Liste belassen, um es später mit aktualisierten Bedrohungssignaturen zu untersuchen, oder es löschen. Diese Aktion kann sowohl auf ein einzelnes Objekt der Liste als auch auf mehrere ausgewählte Objekte angewandt werden.
- **Aus der Liste löschen**. Der Eintrag über den Fund des Objekts wird aus dem Bericht gelöscht.

- **Zur vertrauenswürdigen Zone hinzufügen** – Das Objekt wird den Schutzausnahmen hinzugefügt. Dabei wird ein Fenster mit der Ausnahmeregel für dieses Objekt geöffnet.
- **Alle desinfizieren** – Alle Objekte der Liste desinfizieren. Kaspersky Internet Security versucht, die Objekte unter Verwendung der Bedrohungssignaturen zu bearbeiten.
- **Leeren** – Den Bericht über gefundene Objekte leeren. Dabei verbleiben alle gefundenen gefährlichen Objekte auf Ihrem Computer.
- **Datei anzeigen** – Öffnen von Microsoft Windows Explorer in dem Ordner, in dem sich das Objekt befindet.
- **Auf** http://www.viruslist.de **anschauen** – Zur Beschreibung des Objekts in der Viren-Enzyklopädie auf der Seite von Kaspersky Lab gehen.
- **Auf** www.google.de **nachschauen** – Mit Hilfe der Suchmaschine Informationen über das Objekt suchen.
- **Suche** – Die Bedingungen für die Suche nach einem Objekt (nach Name oder Status) in der Liste angeben.

Außerdem können Sie die Informationen dieses Fensters nach jeder Spalte aufsteigen oder absteigend sortieren.

17.3.1. Konfiguration der Berichtsparameter

Zur Konfiguration der Parameter für das Erstellen und Speichern von Berichten

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security mit dem Link Einstellungen aus dem Programmhauptfenster.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Datenverwaltung**.
3. Nehmen Sie im Block **Berichte** (s. Abb. 81) die erforderlichen Einstellungen vor:
   - Erlauben oder Verbieten Sie das Aufzeichnen von Ereignissen mit rein informativem Charakter im Bericht. In der Regel sind solche Ereignisse nicht für den Schutz wichtig. Aktivieren Sie das Kontrollkästchen ☑ **Informative Ereignisse protokollieren**, um das Speichern solcher Ereignisse zu erlauben.
   - Sie können festlegen, dass nur Ereignisse protokolliert werden, die beim letzten Start der Aufgabe eingetreten sind. Dadurch kann Festplattenplatz gespart werden, weil der Bericht eine

geringere Größe besitzt. Wenn das Kontrollkästchen **Nur aktuelle Ereignisse speichern** aktiviert ist, werden die Informationen im Bericht bei jedem Neustart der Aufgabe aktualisiert. Allerdings werden nur Informationen mit rein informativem Charakter überschrieben.

- Bestimmen Sie, wie lange Berichte gespeichert werden sollen. Der Standardwert für die Speicherdauer von Berichten beträgt 30 Tage. Sie können die Speicherdauer ändern oder diese Beschränkung völlig aufheben.

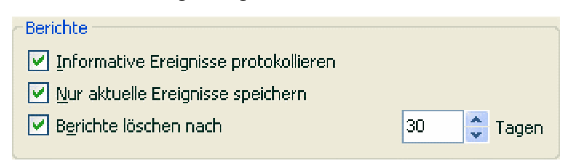


Abbildung 81. Einstellungen für das Erstellen von Berichten

17.3.2. Registerkarte *Gefunden*

Diese Registerkarte (s. Abb. 82) enthält eine Liste der gefährlichen Objekte, die von Kaspersky Internet Security gefunden wurden. Für jedes Objekt werden der vollständige Name und der Status angegeben, der ihm vom Programm bei der Untersuchung/Bearbeitung zugewiesen wurde.

Damit in der Liste nicht nur gefährliche Objekte, sondern auch Objekte, die erfolgreich desinfiziert wurden, angezeigt werden, aktivieren Sie das Kontrollkästchen **Desinfizierte Objekte anzeigen**.

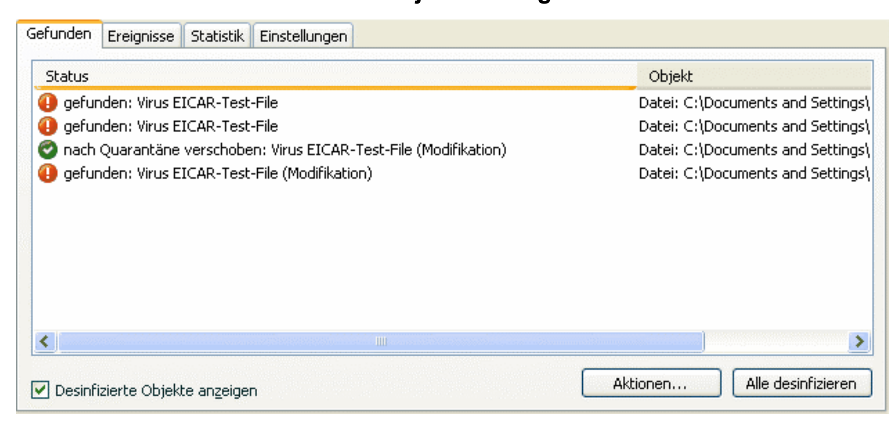


Abbildung 82. Liste der gefundenen gefährlichen Objekte

Die Bearbeitung gefährlicher Objekte, die während der Arbeit von Kaspersky Internet Security gefunden wurden, erfolgt mit Hilfe der Schaltfläche **Desinfizieren** (für ein Objekt oder eine Gruppe ausgewählter Objekte) oder **Alle desinfizieren** (zur Bearbeitung aller Objekte in der Liste). Bei der Bearbeitung jedes Objekts erscheint auf dem Bildschirm eine Meldung, in der Sie aufgefordert werden, über die Aktion mit dem Objekt zu entscheiden.

Wenn Sie im Meldungsfenster das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden** ankreuzen, wird die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewandt, die vor dem Beginn der Bearbeitung in der Liste ausgewählt wurden.

17.3.3. Registerkarte *Ereignisse*

Auf dieser Registerkarte (s. Abb. 83) wird eine vollständige Liste aller wichtigen Ereignisse bei der Arbeit der Schutzkomponente oder beim Ausführen einer Aufgabe zur Virensuche oder zum Update für die Bedrohungssignaturen geführt, wenn dem keine Regel zur Aktivitätskontrolle entgegensteht (s. Pkt. 10.1.1 auf S. 138).

Es gibt folgende Ereignistypen:

Kritische Ereignisse – Ereignisse mit kritischer Priorität, die auf Probleme bei der Arbeit des Programms oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Beispiele: *Virus gefunden*, *Funktionsstörung*.

Wichtige Ereignisse – Ereignisse, die unbedingt beachtet werden müssen, weil Sie wichtige Situationen bei der Programmarbeit wiedergeben. Beispiel: *abgebrochen*.

Informative Ereignisse – Ereignisse mit informativem Charakter, die in der Regel keine wichtigen Informationen enthalten. Beispiele: *ok*, *nicht bearbeitet*. Diese Ereignisse erscheinen nur im Ereignisbericht, wenn das Kontrollkästchen ☑ **Alle Ereignisse anzeigen** aktiviert ist.

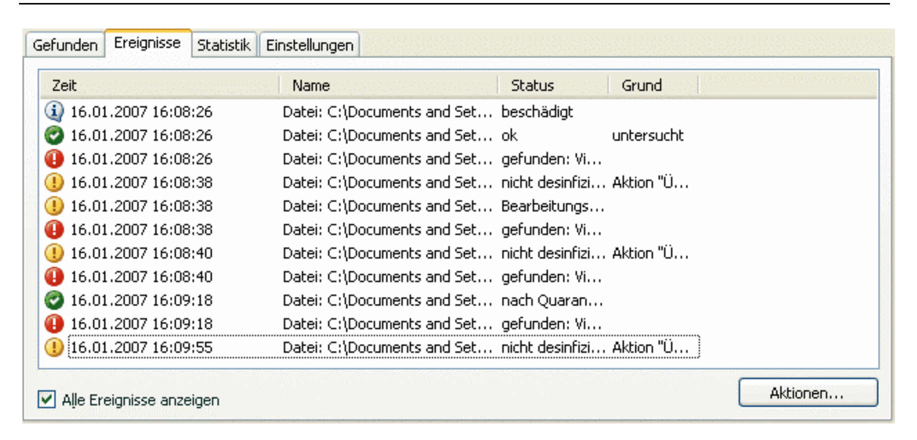


Abbildung 83. Ereignisse, die bei der Arbeit einer Komponente aufgetreten sind

Das Format der im Ereignisbericht enthaltenen Ereignisse kann in Abhängigkeit von der Komponente oder Aufgabe unterschiedlich sein. Für Update-Aufgaben wird beispielsweise angegeben:

- Ereignisname
- Name des Objekts, für das dieses Ereignis aufgezeichnet wurde.
- Zeitpunkt, zu dem das Ereignis eintrat.
- Größe der heruntergeladenen Datei.

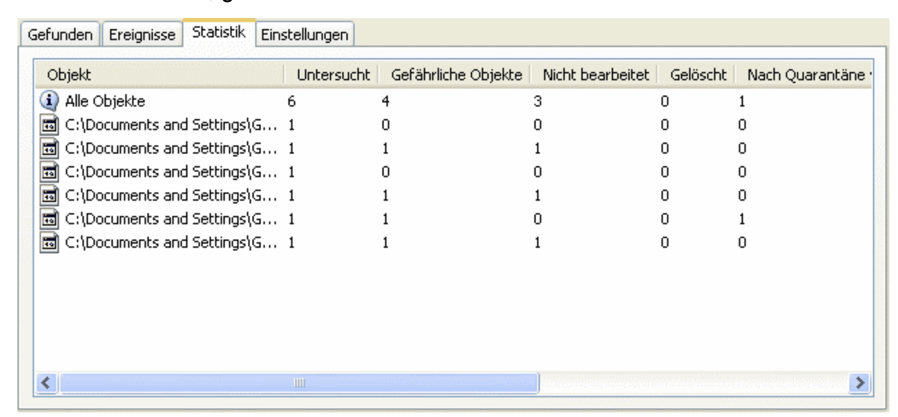
Für eine Aufgabe zur Virensuche enthält der Ereignisbericht den Namen des untersuchten Objekts und den Status, der dem Objekt aufgrund der Untersuchung/Bearbeitung zugewiesen wurde.

Für das Anti-Spam-Training können Sie bei der Ansicht des Berichts dieser Komponente auch das spezielle Kontextmenü verwenden. Wählen Sie dazu den Namen einer E-Mail aus, öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie **Als Spam markieren**, wenn es sich um Spam handelt, oder **Als KEIN Spam markieren**, wenn Sie eine nützliche Mail gewählt haben. Außerdem können Sie auf Basis der Informationen, die aus der E-Mail-Analyse hervorgehen, die schwarze und die weiße Anti-Spam-Liste ergänzen. Verwenden Sie dazu die entsprechenden Punkte des Kontextmenüs.

17.3.4. Registerkarte *Statistik*

Eine ausführliche Statistik über die Arbeit der Komponente oder die Ausführung der Aufgabe zur Virensuche wird auf dieser Registerkarte aufgezeichnet (s. Abb. 84). Hier können Sie erfahren:

- Wie viele Objekte während der laufenden Sitzung der Komponente oder bei der Aufgabenausführung auf das Vorhandensein gefährlicher Objekte untersucht wurden. Außerdem wird die Anzahl der untersuchten Archive, gepackten Dateien, kennwortgeschützten und beschädigten Objekte angegeben.
- Wie viele gefährliche Objekte gefunden wurden. Wie viele davon nicht desinfiziert, gelöscht und in die Quarantäne verschoben wurden.



Objekt	Untersucht	Gefährliche Objekte	Nicht bearbeitet	Gelöscht	Nach Quarantäne
Alle Objekte	6	4	3	0	1
C:\Documents and Settings\G...	1	0	0	0	0
C:\Documents and Settings\G...	1	1	1	0	0
C:\Documents and Settings\G...	1	0	0	0	0
C:\Documents and Settings\G...	1	1	1	0	0
C:\Documents and Settings\G...	1	1	0	0	1
C:\Documents and Settings\G...	1	1	1	0	0

Abbildung 84. Statistik über die Arbeit einer Komponente

17.3.5. Registerkarte *Einstellungen*

Die Registerkarte **Einstellungen** (s. Abb. 85) enthält eine vollständige Übersicht der Parameter, mit denen die Schutzkomponente arbeitet oder die Untersuchungsaufgabe bzw. das Programmupdate ausgeführt wird. Sie können erfahren, welche Schutzstufe die Arbeit der Komponente bietet oder auf welcher Stufe die Virensuche ausgeführt wird, welche Aktion mit einem gefährlichen Objekt ausgeführt wird oder welche Einstellungen beim Programmupdate verwendet werden, usw. Um zur Konfiguration der Parameter zu wechseln, verwenden Sie den Link Einstellungen ändern.

Für die Aufgaben zur Virensuche können zusätzliche Ausführungsbedingungen festgelegt werden:

- Ausführungspriorität der Untersuchungsaufgabe bei Auslastung des Prozessors festlegen. Standardmäßig ist das Kontrollkästchen ☑ **Ressourcen für andere Anwendungen freigeben** aktiviert. Das Programm überwacht dabei das Auslastungsniveau des Prozessors und der Laufwerkssubsysteme im Hinblick auf die Aktivität anderer Anwendungen. Wenn das Auslastungsniveau wesentlich ansteigt und die normale Arbeit der Benutzeranwendungen stört, beendet das Programm

die Aktivität zur Ausführung der Untersuchungsaufgaben. Dies führt zur Verlängerung der Untersuchungszeit und zur Überlassung von Ressourcen an Benutzeranwendungen.

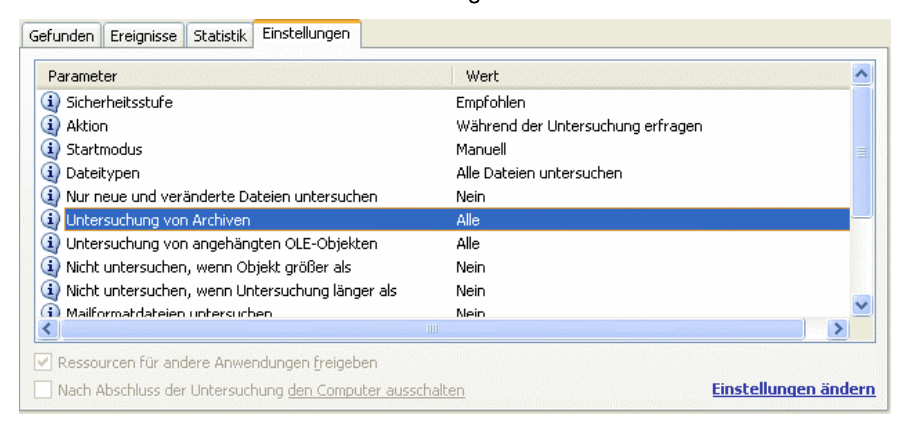


Abbildung 85. Einstellungen für die Arbeit einer Komponente

- Modus für die Arbeit des Computers nach dem Abschluss der Untersuchungsaufgabe bestimmen. Sie können festlegen, das der Computer nach Untersuchungsende ausgeschaltet oder neu gestartet wird oder in den Standbymodus oder Ruhemodus wechselt. Klicken Sie mit der linken Maustaste auf den Hyperlink, bis er den gewünschten Wert annimmt.

  Diese Option ist beispielsweise dann von Nutzen, wenn Sie die Virenuntersuchung des Computers kurz vor Feierabend starten und nicht auf deren Abschluss warten möchten.

  Die Verwendung dieser Option erfordert allerdings folgende zusätzlichen Vorbereitungen: Vor dem Untersuchungsstart muss die Kennwortabfrage bei der Objektuntersuchung deaktiviert werden, falls diese aktiviert war, und der Modus zur automatischen Bearbeitung gefährlicher Objekte muss festgelegt werden. Dadurch wird der interaktive Funktionsmodus des Programms abgeschaltet. Das Programm führt keine Anfragen durch, welche Ihre Reaktion erfordern und den Untersuchungsvorgang unterbrechen.

17.3.6. Registerkarte *Makros*

Alle Makros, deren Ausführung während der laufenden Sitzung von Kaspersky Internet Security versucht wurde, werden auf der Registerkarte **Makros** aufgeführt (s. Abb. 86). Hier werden der vollständige Name jedes Makros, die

Ausführungszeit und der Status, der das Ergebnis der Makrobearbeitung angibt, genannt.

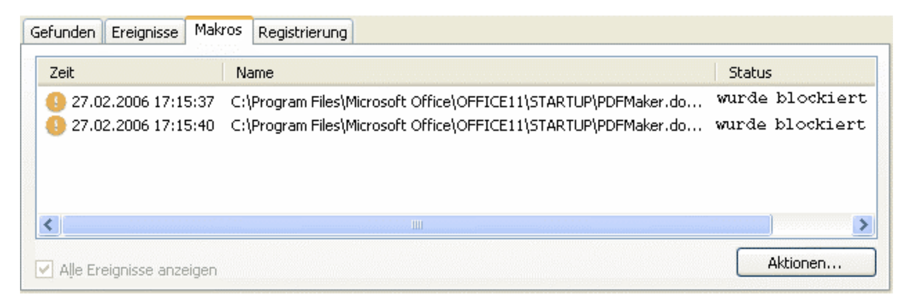


Abbildung 86. Liste der gefundenen gefährlichen Makros

Sie können bestimmen, welche Ereignisse auf dieser Registerkarte des Berichts angezeigt werden sollen. Um die Anzeige informativer Ereignisse abzuschalten, deaktivieren Sie das Kontrollkästchen **Alle Ereignisse anzeigen**.

17.3.7. Registerkarte *Registrierung*

Die Operationen mit Registrierungsschlüsseln, deren Ausführung seit dem Programmstart versucht wurde, werden auf der Registerkarte **Registrierung** (s. Abb. 87) festgehalten, wenn die Protokollierung nicht durch eine Regel untersagt wird (s. Pkt. 10.1.4.2 auf S. 153).

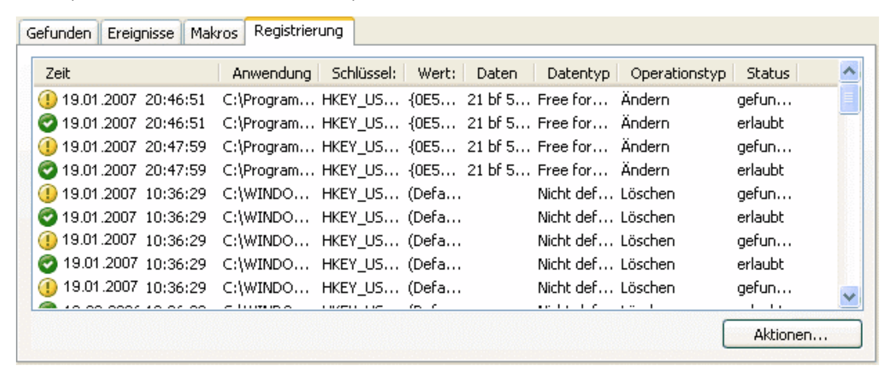


Abbildung 87. Ereignisse, die das Lesen und
die Veränderung der Systemregistrierung betreffen

Auf der Registerkarte werden der vollständige Name, Wert und Datentyp des Schlüssels sowie Angaben über die auszuführende Operation (versuchte Aktion, Zeitpunkt und ob die Aktion erlaubt wurde) angegeben.

17.3.8. Registerkarte *Phishing-Seiten*

Diese Registerkarte des Berichts (s. Abb. 88) enthält alle Versuche zu Phishing-Angriffen, die während der laufenden Sitzung von Kaspersky Internet Security ausgeführt wurden. Für jeden Angriff werden folgende Daten genannt: Link zu der Phishing-Seite, der in der Nachricht oder einer anderen Quelle gefunden wurde, Datum und Uhrzeit zu denen der Angriff erkannt wurde, und Status des Angriffs (blockiert oder nicht blockiert).



Abbildung 88. Blockierte Versuche zu Phishing-Angriffen

17.3.9. Registerkarte *Popup-Fenster*

Die Adressen aller Popup-Fenster, die von Anti-Spy blockiert wurden, werden auf dieser Registerkarte des Berichts genannt (s. Abb. 89). Solche Fenster werden in der Regel auf Webseiten im Internet geöffnet.

Für jedes Popup-Fenster werden folgende Daten aufgezeichnet: Internetadresse, Datum und Uhrzeit zu denen es blockiert wurde.

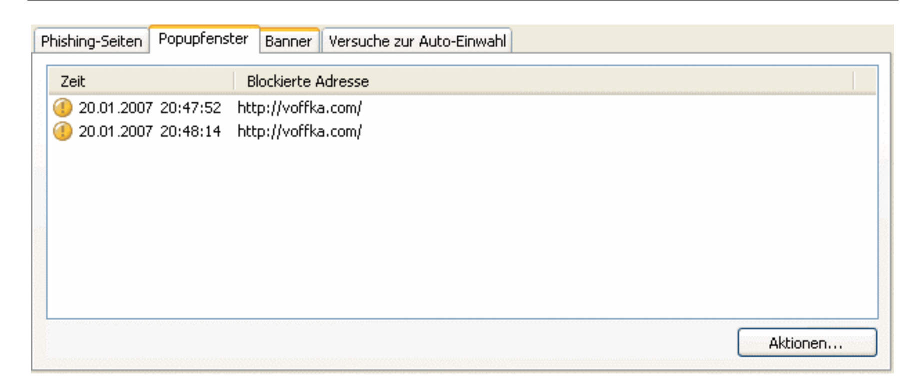


Abbildung 89. Liste der blockierten Popup-Fenster

17.3.10. Registerkarte *Banner*

Die Adressen der Banner, die während der laufenden Sitzung von Kaspersky Internet Security gefunden wurden, werden auf dieser Registerkarte des Berichts angezeigt (s. Abb. 90). Jedes Banner wird durch seine Internetadresse und den Bearbeitungsstatus (erlaubt oder verboten) charakterisiert.

Für verbotene Banner können Sie erlauben, dass diese angezeigt werden. Wählen Sie dazu in der genannten Liste das gewünschte Objekt und verwenden Sie die Schaltfläche **Aktionen** → **Erlauben**.

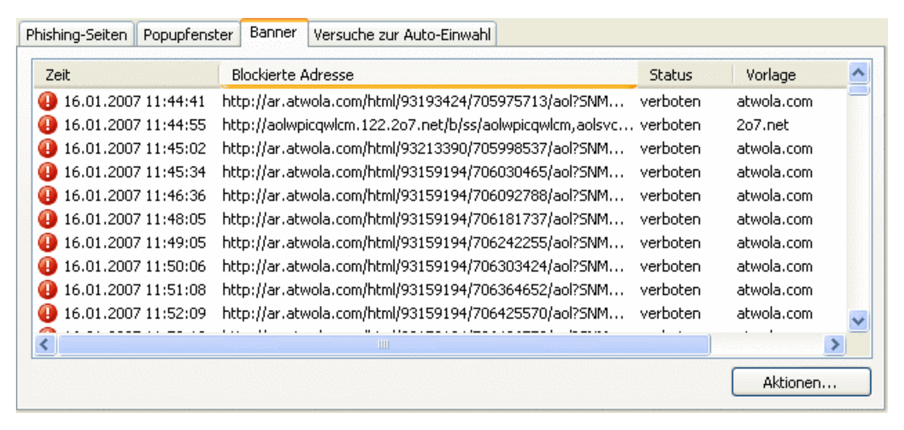


Abbildung 90. Liste der blockierten Banner

17.3.11. Registerkarte *Versuche zur Auto-Einwahl*

Diese Registerkarte (s. Abb. 91) zeigt alle Versuche zur versteckten Einwahl auf kostenpflichtige Webseiten im Internet. Diese Versuche werden in der Regel von schädlichen Programmen ausgeführt, die auf Ihrem Computer installiert sind.

In diesem Bericht können Sie feststellen, von welchem Modul der Auto-Einwahlversuch ausgeführt wurde. Außerdem werden die Nummer, über die versucht wurde eine Internetverbindung herzustellen, der Status des Versuchs (blockiert oder erlaubt) und die Gründe für den Status genannt.

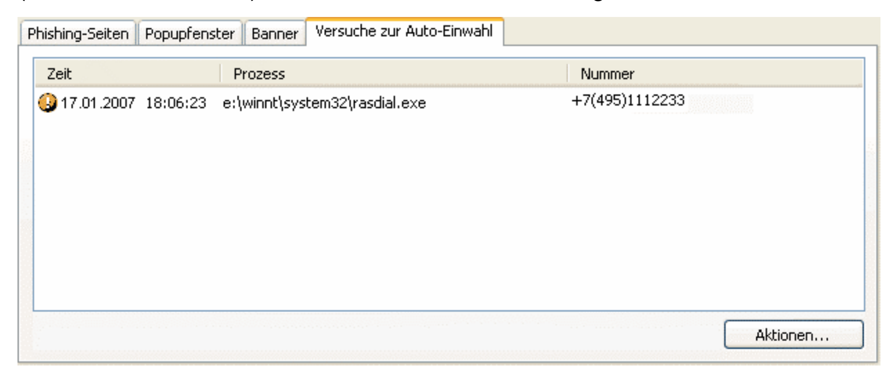


Abbildung 91. Versuche zur versteckten Auto-Einwahl auf kostenpflichtige Ressourcen

17.3.12. Registerkarte *Netzwerkangriffe*

Diese Registerkarte (s. Abb. 92) bietet eine kurze Übersicht der Netzwerkangriffe, die auf Ihren Computer verübt wurden. Diese Informationen werden gespeichert, wenn das Detektionssystem für Angriffe aktiviert ist, das alle Angriffsversuche auf Ihren Computer kontrolliert.

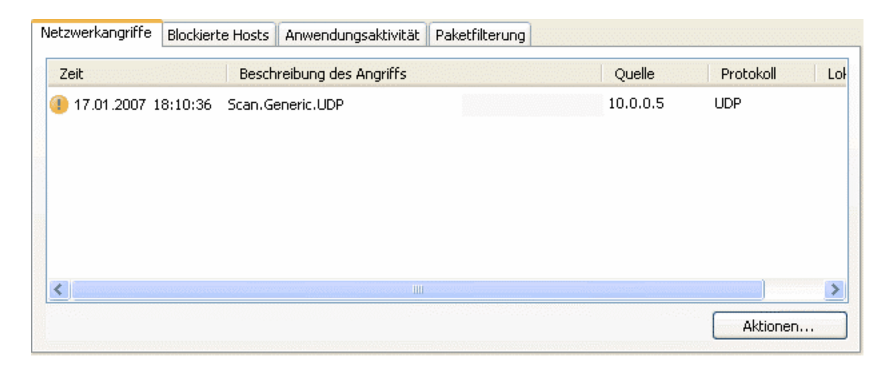


Abbildung 92. Liste der blockierten Netzwerkangriffe

Die Registerkarte *Netzwerkangriffe* enthält folgende Informationen über einen Angriff:

- Quelle des Angriffs (IP-Adresse, Host usw.)
- Nummer des lokalen Ports, auf dem versucht wurde, den Computer anzugreifen.
- Kurze Beschreibung des Angriffs.
- Zeitpunkt, zu dem der Angriffsversuch erfolgte.

Verwenden Sie die Schaltfläche **Aktionen** → **Alle löschen**, um alle Angriffe aus der Liste zu löschen.

17.3.13. Registerkarte *Blockierte Hosts*

Auf dieser Registerkarte des Berichts werden alle Hosts genannt, deren Netzwerkaktivität vom Detektionsmodul für Angriffe aufgrund eines erkannten Angriffs blockiert wurde (s. Abb. 93).

Für jeden Host werden sein Name und der Zeitpunkt genannt, zu dem er blockiert wurde. Auf dieser Registerkarte können Sie einen Host freigeben. Wählen Sie dazu den Host in der Liste aus und klicken Sie auf die Schaltfläche **Aktionen** → **Freigeben**.

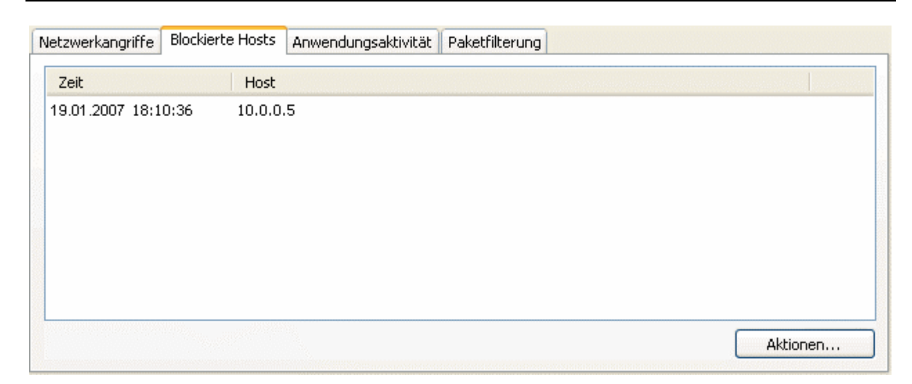


Abbildung 93. Liste der blockierten Hosts

17.3.14. Registerkarte *Anwendungsaktivität*

Wenn bei der Arbeit von Kaspersky Internet Security die Firewall verwendet wird, dann werden auf der Registerkarte **Anwendungsaktivität** alle Anwendungen angezeigt, deren Aktivität unter eine Regel für Anwendungen fällt, falls diese Aktivität während der laufenden Sitzung der Anwendung protokolliert wurde (s. Abb. 94).

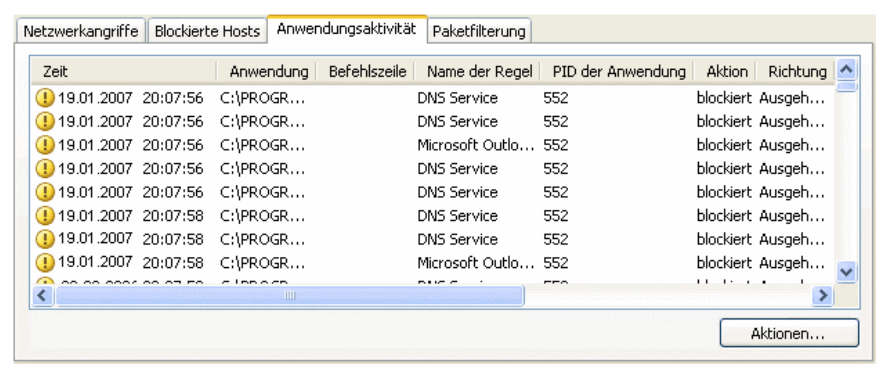


Abbildung 94. Aktivitätskontrolle von Anwendungen

> Die Aktivität wird nur dann protokolliert, wenn in der Regel das Kontrollkästchen ☑ **Protokollieren** aktiviert wurde. In den im Lieferumfang von Kaspersky Internet Security enthaltenen Regeln für Anwendungen ist das Kontrollkästchen standardmäßig nicht aktiviert.

Für jede Anwendung werden die wichtigsten Eigenschaften (Name, PID, Name der Regel) und eine kurze Charakteristik ihrer Aktivität (Protokoll, Richtung des Pakets, usw.) angegeben. Außerdem wird darüber informiert, ob die Aktivität der Anwendung blockiert wurde oder nicht.

17.3.15. Registerkarte *Paketfilterung*

Auf der Registerkarte **Paketfilterung** werden Informationen über Empfang und Übertragung von Paketen angezeigt, die unter eine Filterregel fallen und während der laufenden Sitzung der Anwendung protokolliert wurden (s. Abbildung 95).

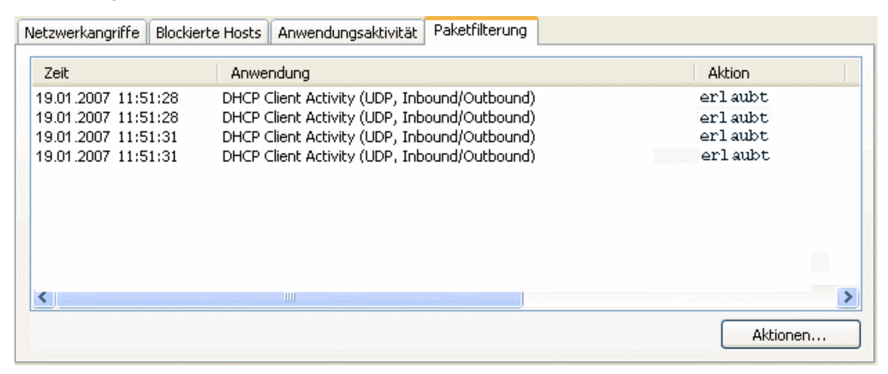


Abbildung 95. Kontrolle von Datenpaketen

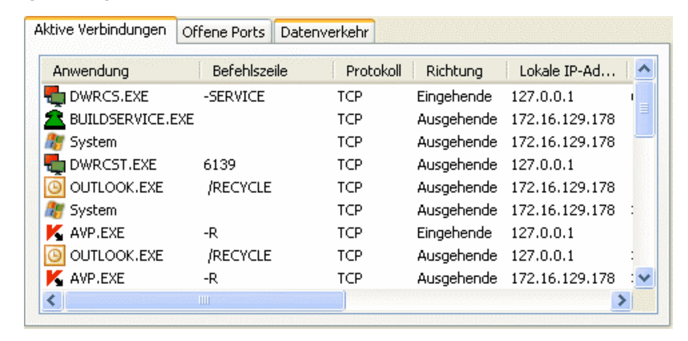
Die Aktivität wird nur dann protokolliert, wenn in der Regel das Kontrollkästchen **Protokollieren** aktiviert wurde. In den Regeln für Pakete, die im Lieferumfang von Kaspersky Internet Security enthalten sind, ist das Kontrollkästchen aktiviert.

Für jedes Paket werden das Ergebnis der Filterung (das Paket wurde blockiert oder nicht), die Richtung des Pakets, das Protokoll und andere Parameter der Netzwerkverbindung für den Empfang/die Übertragung des Pakets angegeben. Außerdem wird darüber informiert, ob die Aktivität der Anwendung blockiert wurde oder nicht.

17.3.16. Registerkarte *Aktive Verbindungen*

Alle aktiven Netzwerkverbindungen, die im Augenblick auf Ihrem Computer bestehen, werden auf der Registerkarte **Aktive Verbindungen** angezeigt (s.

Abb. 96). Für jede Verbindung werden der Name der Anwendung, welche sie initiiert hat, das Protokoll, mit dem die Verbindung ausgeführt wird, die Richtung der Verbindung (eingehend oder ausgehend) und Verbindungsparameter (lokaler und entfernter Port und IP-Adressen) angegeben. Hier können Sie das Volumen der übertragenen/empfangenen Informationen feststellen und wie lange eine Verbindung bereits ausgeführt wird. Für eine ausgewählte Verbindung kann eine Regel erstellt werden. Außerdem kann sie getrennt werden. Verwenden Sie dazu die entsprechenden Punkte des Kontextmenüs, das durch Rechtsklick auf die Verbindungsliste geöffnet wird.



Aktive Verbindungen | Offene Ports | Datenverkehr

Anwendung	Befehlszeile	Protokoll	Richtung	Lokale IP-Ad...
DWRCS.EXE	-SERVICE	TCP	Eingehende	127.0.0.1
BUILDSERVICE.EXE		TCP	Ausgehende	172.16.129.178
System		TCP	Ausgehende	172.16.129.178
DWRCST.EXE	6139	TCP	Ausgehende	127.0.0.1
OUTLOOK.EXE	/RECYCLE	TCP	Ausgehende	172.16.129.178
System		TCP	Ausgehende	172.16.129.178
AVP.EXE	-R	TCP	Eingehende	127.0.0.1
OUTLOOK.EXE	/RECYCLE	TCP	Ausgehende	127.0.0.1
AVP.EXE	-R	TCP	Ausgehende	172.16.129.178

Abbildung 96. Liste der aktiven Verbindungen

17.3.17. Registerkarte *Offene Ports*

Alle Ports, die momentan auf Ihrem Computer für Netzwerkverbindungen geöffnet sind, werden auf der Registerkarte **Offene Ports** angezeigt (s. Abb. 97). Für jeden Port werden seine Nummer, das Datenübertragungsprotokoll, der Name der Anwendung, die den Port benutzt, sowie der Zeitraum, während dem dieser Port für die Verbindung geöffnet war, genannt.

Aktive Verbindungen | Offene Ports | Datenverkehr

Lokale...	Protokoll	Anwendung	Bef...	Lok...	Dauer
1112	TCP	System		0.0.0.0	22:25:14
1350	TCP	System		0.0.0.0	22:08:51
3050	TCP	System		0.0.0.0	05:05:18
135	TCP	SVCHOST.EXE	-K RP...	0.0.0.0	22:35:34
1025	UDP	SVCHOST.EXE	-K NE...	0.0.0.0	22:35:31
1026	UDP	SVCHOST.EXE	-K NE...	0.0.0.0	22:35:31
2201	UDP	SVCHOST.EXE	-K NE...	0.0.0.0	00:00:44
1027	UDP	LSASS.EXE		127.0...	22:35:31
500	UDP	LSASS.EXE		0.0.0.0	22:35:25
4500	UDP	LSASS.EXE		0.0.0.0	22:35:25

Abbildung 97. Liste der auf dem Computer geöffneten Ports

Diese Informationen können beispielsweise während Epidemien und Netzwerkangriffen nützlich sein, wenn bekannt ist, welcher Port von Angreifern verwendet wird. Sie können feststellen, ob dieser Port auf Ihrem Computer geöffnet ist und die erforderlichen Maßnahmen zum Schutz Ihres Computers einleiten (beispielsweise den Angriffsdetektor aktivieren, den bedrohten Port schließen oder eine Regel für ihn erstellen).

17.3.18. Registerkarte *Datenverkehr*

Auf dieser Registerkarte (s. Abb. 98) befinden sich Informationen über alle eingehenden und ausgehenden Verbindungen, die zwischen Ihrem Computer und anderen Computern hergestellt worden sind (einschließlich Webservern, Mailservern usw.). Für jede Verbindung werden folgende Daten genannt: Name und IP-Adresse des Hosts, mit dem eine Verbindung stattfand, sowie Volumen des eingehenden und ausgehenden Datenverkehrs.

Aktive Verbindungen | Offene Ports | Datenverkehr

Host	IP-Adresse	Empfangen	Gesendet
192.168...	172.16.1.67	1.9 KB	0 Bytes
luthaxp....	172.16.1.68	525 Bytes	0 Bytes
192.168...	172.16.12...	83.4 KB	53.2 KB
192.168...	192.168.1...	1 KB	2.8 KB
kav6_9...	172.16.2.70	525 Bytes	0 Bytes
tl-dozer...	172.16.12...	34.9 KB	23.6 KB
192.168...	192.168.1...	186 Bytes	558 Bytes
tl-comp...	172.16.2.73	1 KB	0 Bytes
tl-p4d-2...	172.16.1.74	525 Bytes	0 Bytes
192.168...	172.16.10...	2 KB	0 Bytes
192.168...	172.16.4.71	525 Bytes	324 Bytes

Abbildung 98. Datenverkehr der aktiven Netzwerkverbindungen

17.4. Allgemeine Informationen über die Anwendung

Allgemeine Informationen über das Programm finden Sie im Abschnitt **Service** des Hauptfensters (s. Abb. 99).

Die Informationen sind in drei Blöcke unterteilt:

- Der Abschnitt **Informationen zum Programm** informiert über Programmversion, Datum der letzten Aktualisierung und Anzahl der momentan bekannten Bedrohungen.
- Kurze Informationen über das auf Ihrem Computer installierte Betriebssystem befinden sich im Block **Informationen zum System**.

- Die wichtigsten Informationen über die von Ihnen erworbene Lizenz zur Nutzung von Kaspersky Internet Security befinden sich im Block **Informationen zur Lizenz**.



Abbildung 99. Informationen zu Programm, Programmlizenz und Betriebssystem

Bei einer Kontaktaufnahme mit dem technischen Support-Service von Kaspersky Lab benötigen Sie alle genannten Informationen (s. Pkt. 17.5 auf S. 283).

17.5. Lizenzverwaltung

Die Möglichkeit zur Nutzung von Kaspersky Internet Security wird durch das Vorhandensein eines *Lizenzschlüssels* bestimmt. Den Schlüssel erhalten Sie durch den Kauf des Produkts und er berechtigt Sie ab dem Tag der Installation des Schlüssels zur Nutzung der Anwendung.

Ist kein Lizenzschlüssel vorhanden und die Anwendung wurde nicht als Testversion aktiviert, dann funktioniert Kaspersky Internet Security im Modus, in dem nur ein einziges Update möglich ist. Danach können keine weiteren Aktualisierungen vorgenommen werden.

Wenn eine Testversion der Anwendung aktiviert wurde, stellt Kaspersky Internet Security nach Ablauf der Testdauer seine Funktion ein.

Mit Ablauf der Gültigkeitsdauer einer kommerziellen Lizenz bleibt die Funktionalität des Programms unter Ausnahme der Updatemöglichkeit für die Bedrohungssignaturen erhalten. Sie können Ihren Computer mit Hilfe der Untersuchungsaufgaben weiterhin auf das Vorhandensein von Viren untersuchen und die Schutzkomponenten verwenden, allerdings nur mit den Bedrohungssignaturen, die bei Ablauf der Lizenzgültigkeit aktuell waren. Demzufolge können wir Ihnen keinen hundertprozentigen Schutz vor neuen Viren garantieren, die nach dem Ende der Lizenzgültigkeit für das Programm auftreten.

Um eine Infektion Ihres Computers durch neue Viren zu verhindern, empfehlen wird Ihnen, die Lizenz für die Benutzung von Kaspersky Internet Security zu verlängern. Zwei Wochen vor Ablauf der Lizenzgültigkeit werden Sie vom Programm darüber benachrichtigt. Innerhalb dieser zwei Wochen wird bei jedem Programmstart eine entsprechende Meldung auf dem Bildschirm angezeigt.

Um die Lizenz zu verlängern, ist es erforderlich, einen neuen Lizenzschlüssel für Kaspersky Internet Security zu kaufen und zu installieren oder einen Aktivierungscode für die Anwendung anzugeben. Gehen Sie dazu folgendermaßen vor:

Setzen Sie sich mit der Firma in Verbindung, bei der Sie das Produkt gekauft haben, und erwerben Sie einen Lizenzschlüssel für die Nutzung der Anwendung oder einen Aktivierungscode.

oder:

Erwerben Sie direkt bei Kaspersky Lab einen Lizenzschlüssel oder einen Aktivierungscode. Verwenden Sie dazu im Fenster zur Lizenzverwaltung den Hyperlink Lizenz kaufen (s. Abb. 100). Füllen Sie das entsprechende Formular auf der dadurch automatisch geöffneten Webseite aus. Nach Eingang der Bezahlung wird Ihnen an die im Formular angegebene E-Mail-Adresse ein Link zugeschickt. Mit Hilfe des Links können Sie einen Lizenzschlüssel herunterladen oder einen Aktivierungscode für die Anwendung erhalten.

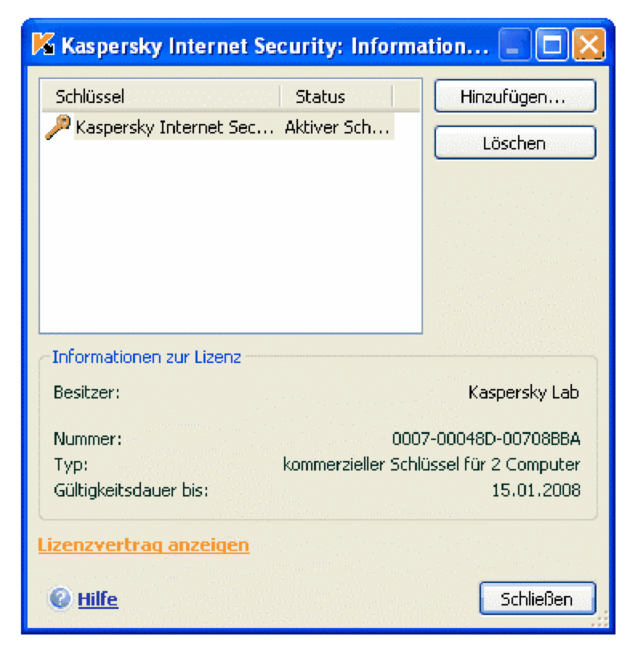


Abbildung 100. Informationen zur Lizenz

Informationen zum verwendeten Lizenzschlüssel befinden sich im Block **Informationen zur Lizenz** des Abschnitts **Service** im Anwendungshauptfenster. In das Fenster zur Lizenzverwaltung gelangen Sie durch Linksklick an eine beliebige Stelle des Blocks. Im folgenden Fenster finden Sie Informationen über den aktiven Schlüssel und können einen Schlüssel hinzufügen oder löschen.

Durch die Auswahl eines Schlüssels in der Liste des Blocks **Informationen zur Lizenz** werden Daten über Nummer, Typ und Gültigkeitsdatum der Lizenz angezeigt. Um einen neuen Lizenzschlüssel hinzuzufügen, verwenden Sie die Schaltfläche **Hinzufügen** und aktivieren Sie die Anwendung mit Hilfe des **Aktivierungsassistenten** (s. Pkt. 3.2.2 auf S. 40). Um einen Schlüssel aus der Liste zu löschen, klicken Sie auf die Schaltfläche **Löschen**.

Zur Anzeige der Bedingungen des Lizenzvertrags für die Benutzung des Produkts dient der Link Lizenzvertrag anzeigen. Um mit Hilfe des Webformulars auf der Kaspersky-Lab-Seite eine Lizenz zu erwerben, klicken Sie auf den Link Lizenz kaufen.

17.6. Technischer Support für Benutzer

Kaspersky Internet Security bietet Ihnen ein breites Spektrum von Möglichkeiten zur Lösung von Fragen und Problemen, die mit der Arbeit des Programms verbunden sind. Alle entsprechenden Optionen finden Sie unter **Support** (s. Abb. 101) im Abschnitt **Service**.



Abbildung 101. Informationen zum technischen Kundendienst

Abhängig vom Problem, das Sie lösen möchten, bieten wir Ihnen an, folgende Leistungen des technischen Supports zu verwenden:

Benutzerforum. Diese Ressource ist ein spezieller Bereich der Kaspersky-Lab-Webseite und enthält Fragen, Kommentare und Vorschläge der Programmbenutzer. Sie können die wichtigsten Themen des Forums kennen lernen, eigene Beiträge über die Anwendung beisteuern oder Antworten auf Ihre Frage finden.

Um zu dieser Ressource zu gelangen, verwenden Sie den Link Benutzerforum.

Wissensdatenbank. Auch diese Ressource ist eine separate Webseite von Kaspersky Lab und enthält Tipps des technischen Support-Service über die Arbeit mit Kaspersky-Lab-Produkten und Antworten auf häufige Fragen. Versuchen Sie, über diese Ressource eine Antwort auf Ihre Frage oder die Lösung Ihres Problems zu finden.

Um technische Online-Unterstützung zu erhalten, verwenden Sie den Link Wissensdatenbank.

Feedback über die Arbeit des Programms. Dieser Dienst dient dazu, um eine ausführliche Beurteilung der Programmarbeit abzugeben oder ein Problem bei der Programmarbeit zu beschreiben. Füllen Sie das spezielle Formular auf der Webseite aus und beschreiben Sie die Situation genau. Um ein Problem genau zu untersuchen, benötigen die Kaspersky-Lab-Spezialisten bestimmte Informationen über Ihr System. Sie können die Systemkonfiguration selbständig beschreiben oder eine Funktion zum automatischen Sammeln von Informationen über Ihren Computer verwenden.

Um zum Formular für die Programmbeurteilung bzw. zur Problembeschreibung zu gelangen, verwenden Sie den Link Senden Sie uns einen Fehlerbericht oder Ihre Meinung.

Hilfe des technischen Supports. Wenn Sie bei der Arbeit mit Kaspersky Internet Security Hilfe benötigen, verwenden Sie den Link, der sich im Block **Lokaler Technischer Support-Service** befindet. Dadurch wird die Kaspersky-Lab-Webseite geöffnet, auf der Sie genaue Informationen darüber finden, wie Sie Hilfe von unseren Spezialisten erhalten können.

17.7. Erstellen einer Liste der zu kontrollierenden Ports

Bei der Arbeit von Schutzkomponenten wie Mail-Anti-Virus, Web-Anti-Virus, Anti-Spy und Anti-Spam werden Datenströme kontrolliert, die mit bestimmten Protokollen übertragen und über bestimmte offene Ports Ihres Computers weitergeleitet werden. Mail-Anti-Virus analysiert beispielsweise die Informationen, die mit dem Protokoll SMTP übertragen werden, Web-Anti-Virus analysiert HTTP-Pakete.

Eine Liste der Ports, die gewöhnlich zur Übertragung von E-Mail und HTTP-Datenströmen benutzt werden, gehört zum Lieferumfang des Programms. Sie können einen neuen Port hinzufügen oder die Kontrolle eines bestimmten Ports

deaktivieren und dadurch veranlassen, dass der Datenstrom, der über diesen Port geleitet wird, nicht auf gefährliche Objekte hin untersucht wird.

Gehen Sie folgendermaßen vor, um die Liste der zu kontrollierenden Ports zu bearbeiten:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security über den Link Einstellungen des Hauptfensters.
2. Wählen Sie **Netzwerkeinstellungen** im Abschnitt **Service** der Konfigurationsstruktur des Programms.
3. Klicken Sie auf der rechten Seite des Konfigurationsfensters auf die Schaltfläche **Port-Einstellungen**.
4. Korrigieren Sie im folgenden Fenster die Liste der zu kontrollierenden Ports (s. Abb. 102).

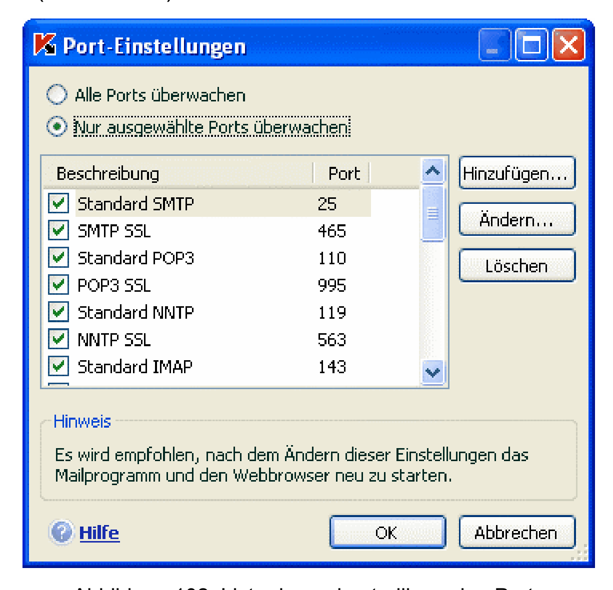


Abbildung 102. Liste der zu kontrollierenden Ports

Dieses Fenster enthält eine Liste der Ports, die von Kaspersky Internet Security kontrolliert werden. Wählen Sie die Variante **Alle Ports überwachen**, damit alle offenen Ports des Netzwerks überwacht werden, oder wählen Sie **Nur ausgewählte Ports überwachen**, um die Liste der zu kontrollierenden Ports selbst anzupassen.

Um einen neuen Port zur Liste der zu kontrollierenden Ports hinzuzufügen,

1. Klicken Sie im Fenster zur Port-Konfiguration auf die Schaltfläche **Hinzufügen**.
2. Geben Sie in den entsprechenden Feldern des Fensters **Neuer Port** die Portnummer und seine Beschreibung an.

Auf Ihrem Computer kann beispielsweise ein nicht standardmäßiger Port für den Datentransfer mit einem entfernten Computer über das HTTP-Protokoll konfiguriert sein. Die Kontrolle des HTTP-Datenverkehrs erfolgt durch die Komponente Web-Anti-Virus. Damit dieser Datenverkehr auf das Vorhandensein von schädlichem Code analysiert wird, muss dieser Port zur Liste der zu kontrollierenden Ports hinzugefügt werden.

Beim Start einer beliebigen Komponente öffnet das Programm Kaspersky Internet Security zur Überwachung aller eingehenden Verbindungen den Port 1110. Wenn dieser Port gerade von einer anderen Anwendung besetzt ist, wird Port 1111, 1112 usw. zur Überwachung gewählt.

Wenn das Programm Kaspersky Internet Security gleichzeitig mit der Firewall eines anderen Herstellers verwendet wird, müssen in den Einstellungen dieser Firewall Erlaubnisregeln für den Prozess *avp.exe* (interner Prozess von Kaspersky Internet Security) für alle aufgezählten Ports erstellt werden.

Beispielsweise kann in Ihrer Firewall eine Regel für den Prozess *iexplorer.exe* vorhanden sein, nach welcher diesem Prozess erlaubt wird, einen Verbindung auf Port 80 herzustellen.

Trotzdem fängt Kaspersky Internet Security die Anfrage für eine Verbindung ab, die vom Prozess *iexplorer.exe* auf Port 80 initiiert wird, und übergibt sie dem Prozess *avp.exe*, der versucht seinerseits eine Verbindung mit der aufgerufenen Webseite herzustellen. Wenn für den Prozess *avp.exe* keine Erlaubnisregel vorhanden ist, wird diese Anfrage von der Firewall blockiert und der Benutzer erhält keinen Zugriff auf die Webseite.

17.8. Untersuchung von SSL-Verbindungen

Eine Verbindung unter Verwendung des SSL-Protokolls bietet den Schutz des Kommunikationskanals im Internet. Das SSL-Protokoll erlaubt die Identifikation der beteiligten Partner, die Daten austauschen. Dazu dienen elektronische Zertifikate. Außerdem werden die zu übertragenden Daten verschlüsselt und die Datenintegrität beim Übertragungsvorgang wird gewährleistet.

Diese Besonderheiten des Protokolls werden von Angreifern zur Verbreitung von schädlichen Programmen benutzt, weil die meisten Antivirenprodukte den SSL-Verkehr nicht untersuchen.

Kaspersky Internet Security bietet die Möglichkeit zur Virenuntersuchung des Datenstroms nach dem SSL-Protokoll. Beim Versuch zur Verbindung mit einer Webressource im sicheren Modus erscheint auf dem Bildschirm eine Meldung (s. Abbildung 103) mit einer Aktionsanfrage an den Benutzer.

Die Meldung enthält Informationen über das Programm, das die Verbindung im geschützten Modus initiiert hat, sowie die Remoteadresse und den Remoteport. Sie werden aufgefordert zu entscheiden, ob die Virenuntersuchung dieser Verbindung erforderlich ist:

- **Bearbeiten** – Bei der Verbindung mit einer Webressource im geschützten Modus den Datenverkehr auf Viren untersuchen.

  Wir empfehlen Ihnen ausdrücklich, die Untersuchung des SSL-Datenverkehrs dann vorzunehmen, wenn Sie sich in einer verdächtigen Webressource befinden oder wenn beim Wechsel auf eine andere Webseite die Datenübertragung mit SSL-Protokoll beginnt. Dies deutet mit hoher Wahrscheinlichkeit auf die Übertragung eines Schadprogramms mit Hilfe des Sicherheitsprotokolls hin.

- **Überspringen** - Die Verbindung mit einer Webressource im geschützten Modus fortsetzen, ohne den Datenverkehr auf Viren zu untersuchen.

Damit die ausgewählte Aktion in Zukunft auf alle Versuche zum Aufbau von SSL-Verbindungen angewandt wird, aktivieren Sie das Kontrollkästchen ☑ **Auf alle anwenden**.



Abbildung 103. Meldung über den Fund einer SSL-Verbindung

Zur Untersuchung von verschlüsselten Verbindungen tauscht Kaspersky Internet Security das angeforderte Sicherheitszertifikat durch ein von ihm signiertes Zertifikat aus. In einigen Fällen akzeptieren Programme, die eine Verbindung herstellen, dieses Zertifikat nicht und die Verbindung kann deshalb nicht hergestellt werden. Wir empfehlen, die Untersuchung des SSL-Datenstroms in folgenden Fällen auszuschalten:

- Bei einer Verbindung mit einer vertrauenswürdigen Webressource, beispielsweise mit der Webseite Ihrer Bank, auf der Sie Ihr eigenes Konto verwalten. In diesem Fall ist es wichtig, eine Bestätigung über die Echtheit des Bankzertifikats zu erhalten.
- Wenn das Programm, das eine Verbindung herstellt, eine Zertifikatsprüfung bei der angefragten Webressource vornimmt. Beispielsweise prüft das Programm MSN Messenger beim Aufbau einer geschützten Verbindung mit einem Server die Echtheit der digitalen Microsoft Corporation-Signatur.

Die Untersuchung von SSL-Verbindungen wird auf der Registerkarte **Netzwerkeinstellungen** im Konfigurationsfenster der Anwendung angepasst:

- **Alle geschützten Verbindungen untersuchen** – den gesamten Datenstrom, der mit dem SSL-Protokoll übertragen wird, auf Viren untersuchen.
- **Beim Fund einer neuen geschützten Verbindung fragen** – Der Benutzer wird jedes Mal nach den gewünschten Aktionen gefragt, wenn versucht wird, eine SSL-Verbindung aufzubauen.

- **Geschützte Verbindungen nicht untersuchen** – den Datenstrom, der mit dem SSL-Protokoll übertragen wird, nicht auf Viren untersuchen.

17.9. Konfiguration der Oberfläche von Kaspersky Internet Security

Kaspersky Internet Security bietet die Möglichkeit, das Aussehen des Programms zu verändern. Dazu können unterschiedliche grafische Elemente und Farbpaletten erstellt und verwendet werden. Zusätzlich besteht die Möglichkeit, aktive Elemente der Benutzeroberfläche anzupassen. Dazu zählen das Programmsymbol im Infobereich der Taskleiste und Popup-Meldungen.

Gehen Sie folgendermaßen vor, um die Programmoberfläche anzupassen:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Internet Security über den Link Einstellungen des Hauptfensters.
2. Wählen Sie **Ansicht** im Abschnitt **Service** der Konfigurationsstruktur des Programms (s. Abb. 104).

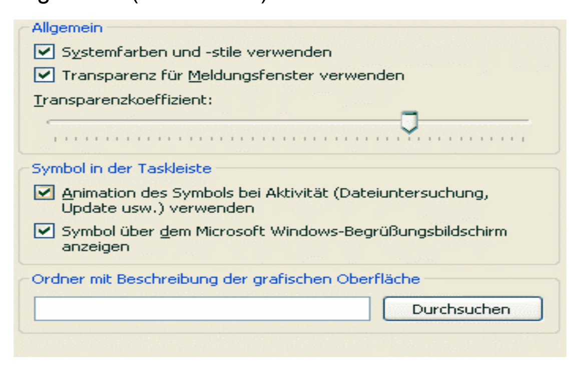


Abbildung 104. Einstellungen für die Programmoberfläche

Auf der rechten Seite des Konfigurationsfensters können Sie festlegen:

- ob der Schutzindikator von Kaspersky Internet Security beim Start des Betriebssystems angezeigt werden soll oder nicht.

  Standardmäßig erscheint dieser Indikator in der rechten oberen Bildschirmecke, wenn das Programm gestartet wird. Er informiert darüber, dass der Schutz Ihres Computers vor jeder Art von Bedrohung

aktiviert ist. Wenn Sie den Schutzindikator nicht verwenden möchten, deaktivieren Sie das Kontrollkästchen ☑ **Symbol über dem Microsoft Windows-Begrüßungsbildschirm anzeigen**.

- ob das Programmsymbol im Infobereich der Taskleiste animiert werden soll oder nicht.

  In Abhängigkeit von der ausgeführten Programmaktion ändert sich das Symbol im Infobereich. Wird beispielsweise die Untersuchung eines Skripts ausgeführt, dann erscheint im Hintergrund des Symbols ein kleines Piktogramm mit einem Skript. Bei der Untersuchung einer E-Mail-Nachricht erscheint das Piktogramm eines Briefs. Die Animation des Programmsymbols wird standardmäßig verwendet. Wenn Sie keine Animation wünschen, deaktivieren Sie das Kontrollkästchen ☑ **Animation des Symbols bei Aktivität verwenden**. In diesem Fall gibt das Symbol nur den Schutzstatus Ihres Computers wieder: Wenn der Schutz aktiviert ist, ist das Symbol farbig. Wenn der Schutz angehalten oder abgeschaltet wurde, nimmt das Symbol graue Farbe an.

- Transparenzstufe der Popup-Meldungen.

  Alle Operationen von Kaspersky Internet Security, die Ihre sofortige Aufmerksamkeit oder Entscheidung erfordern, besitzen das Aussehen einer Popup-Meldung über dem Programmsymbol im Infobereich. Die Meldungsfenster sind halbtransparent, damit sie Ihre Arbeit nicht stören. Wenn der Mauscursor auf das Meldungsfenster geführt wird, wird die Transparenz aufgehoben. Sie können die Transparenzstufe solcher Meldungen ändern. Verschieben Sie dazu den Zeiger auf der Skala **Transparenzkoeffizient** an die gewünschte Position. Deaktivieren Sie das Kontrollkästchen ☑ **Transparenz für Meldungsfenster verwenden**, wenn die Meldungen ohne Transparenz angezeigt werden sollen.

  > Diese Option steht nicht zur Verfügung, wenn die Anwendung auf einem Computer mit dem Betriebssystem Microsoft Windows 98/NT 4.0/ME installiert ist.

- Verwendung eigener grafischer Elemente und Farbpaletten auf der Programmoberfläche.

  Alle auf der Oberfläche von Kaspersky Internet Security verwendeten Farben, Schriften, Piktogramme und Texte können verändert werden. Sie können eine individuelle grafische Oberfläche für das Programm erstellen und es in einer anderen Sprache lokalisieren. Um eine grafische Oberfläche zu verbinden, geben Sie das Verzeichnis mit ihren Parametern im Feld **Ordner mit Beschreibung der grafischen Oberfläche** an. Verwenden Sie zur Auswahl des Verzeichnisses die Schaltfläche **Durchsuchen**.

Standardmäßig werden für die grafische Programmoberfläche die Systemfarben und -stile verwendet. Sie können diese verwerfen. Deaktivieren Sie dazu das Kontrollkästchen ☑ **Systemfarben und –stile verwenden**. In diesem Fall werden die Schemen verwendet, die Sie bei der Konfiguration des Bildschirmdesigns angegeben haben.

Beachten Sie, dass Änderungen der Interfaceparameter von Kaspersky Internet Security beim Wiederherstellen der Standardeinstellungen oder bei der Deinstallation der Anwendung nicht gespeichert werden.

17.10. Notfall-CD zur Systemwiederherstellung

Das Programm Kaspersky Internet Security enthält einen Dienst zum Erstellen einer Notfall-CD zur Systemwiederherstellung.

Die Notfall-CD soll zur Wiederherstellung der Funktionsfähigkeit des Systems nach einem Virusangriff dienen, durch den Systemdateien des Betriebssystems beschädigt wurden und der Computer nicht mehr hochgefahren werden kann. Die Notfall-CD enthält:

- Systemdateien für Microsoft Windows XP Service Pack 2
- eine Auswahl von Dienstprogrammen zur Betriebssystemdiagnose
- Dateien des Programms Kaspersky Internet Security
- Dateien, welche die Bedrohungssignaturen enthalten

Um eine Notfall-CD zu erstellen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie **Notfall-CD** im Abschnitt **Service**.
2. Klicken Sie auf die Schaltfläche **Assistent starten**, um den Vorgang zum Erstellen der Notfall-CD einzuleiten.

Die Notfall-CD dient ausschließlich für den Computer, auf welchem sie erstellt wurde. Die Verwendung der CD auf anderen Computern kann unvorhersehbare Folgen haben, weil sie Informationen über die Parameter des konkreten Computers enthält (z.B. Informationen über Bootsektoren).

Die Option zum Erstellen einer Notfall-CD ist nur verfügbar, wenn die Anwendung auf einem Computer mit dem Betriebssystem Microsoft Windows XP oder Microsoft Windows Vista installiert ist. Auf Computern mit anderen unterstützten Systemen, darunter auch Microsoft Windows XP Professional x64 Edition und Microsoft Windows Vista x64, ist das Erstellen der CD nicht vorgesehen.

17.10.1. Erstellen einer Notfall-CD

Achtung! Zum Erstellen einer Notfall-CD müssen Sie über eine Installations-CD für Microsoft Windows XP Service Pack 2 verfügen.

Die Notfall-CD wird mit Hilfe des Spezialprogramms **PE Builder** erstellt.

Um mit Hilfe von PE Builder eine Notfall-CD zu erstellen, muss dieses Programm vorher auf dem Computer installiert werden.

Beim Erstellen der Notfall-CD werden Sie von einem speziellen Assistenten begleitet, der aus einer Reihe von Fenstern (Schritten) besteht. Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Weiter** und **Zurück**, zum Abschluss der Arbeit des Assistenten die Schaltfläche **Fertig stellen**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Schritt 1. Vorbereitung zum Schreiben

Um die Notfall-CD für die Systemwiederherstellung zu erstellen, geben Sie die Pfade der folgenden Ordner an:

- Installationsorder des Programms von PE Builder.
- Ordner, in dem die Dateien für die Notfall-CD vor dem Schreiben der CD gespeichert werden sollen.

  Wenn Sie nicht zum ersten Mal eine Notfall-CD erstellen, enthält dieser Ordner bereits eine Auswahl von Dateien, die beim vorigen Mal gespeichert wurden. Aktivieren Sie das entsprechende Kontrollkästchen, um die früher gespeicherten Dateien zu verwenden.

> Beachten Sie, dass die früher gespeicherte Version der Notfall-CD-Dateien veraltete Bedrohungssignaturen enthält. Um die Virenanalyse des Computers und die Systemwiederherstellung auf optimale Weise zu gewährleisten, wird empfohlen, die Bedrohungssignaturen zu aktualisieren und eine neue Version der Notfall-CD zu erstellen.

- Installations-CD für Microsoft Windows XP Service Pack 2.

Klicken Sie auf die Schaltfläche **Weiter**, nachdem Sie die erforderlichen Pfadangaben gemacht haben. Dadurch wird das Programm PE Builder gestartet und der Vorgang zum Erstellen der Dateien für die Notfall-CD beginnt. Warten Sie, bis der Vorgang abgeschlossen wird. Dies kann einige Minuten in Anspruch nehmen.

Schritt 2. Erstellen einer ISO-Datei

Nachdem das Programm PE Builder die Dateien für die Notfall-CD vorbereitet hat, wird das Fenster **Erstellen der ISO-Datei** geöffnet.

Die ISO-Datei ist ein Image der zu erstellenden Notfall-CD in Form eines Archivs. Dateien im ISO-Format werden von den meisten CD-Brennprogrammen (beispielsweise Nero) unterstützt.

Wenn Sie nicht zum ersten Mal eine Notfall-CD erstellen, können Sie die Verwendung der vorherigen Version der ISO-Datei wählen. Wählen Sie dazu die Variante **Vorhandene ISO-Datei verwenden**.

Schritt 3. Schreiben der CD

In diesem Fenster fordert der Assistent Sie auf anzugeben, wann die Dateien der Notfall-CD auf die CD geschrieben werden sollen: jetzt oder später.

Wenn Sie das unverzügliche Schreiben der CD wählen, geben Sie an, ob der Inhalt der CD vor dem Schreiben gelöscht werden soll. Aktivieren Sie dazu das entsprechende Kontrollkästchen. Diese Option steht nur zur Verfügung, wenn die CD wiederholt mit Daten beschrieben werden kann (CD-RW).

Durch Klick auf die Schaltfläche **Weiter** wird der Vorgang zum Schreiben der Notfall-CD gestartet. Warten Sie bis zum Abschluss des Vorgangs. Dies kann einige Minuten in Anspruch nehmen.

Schritt 4. Abschluss des Erstellens der Notfall-CD

In diesem Fenster informiert der Assistent Sie darüber, dass die Notfall-CD erfolgreich erstellt wurde.

17.10.2. Verwendung der Notfall-CD

Beachten Sie, dass Kaspersky Internet Security im Notfall-Modus zur Systemwiederherstellung nur arbeitet, wenn das Hauptfenster geöffnet ist. Beim Schließen des Programmhauptfensters wird das Programm beendet.

In dem Programm Bart PE, das standardmäßig installiert wird, werden keine chm-Dateien und Webbrowser unterstützt. Deshalb stehen im Notfall-Modus zur Systemwiederherstellung das Hilfesystem von Kaspersky Internet Security und die Links auf der Programmoberfläche nicht zur Verfügung.

Sollte eine Situation eintreten, in der das Betriebssystem aufgrund eines Virusangriffs nicht mehr gestartet werden kann, dann gehen Sie folgendermaßen vor:

1. Erstellen Sie unter Verwendung des Programms Kaspersky Internet Security auf einem virusfreien Computer eine Notfall-CD.
2. Legen Sie die Notfall-CD in das CD-Laufwerk des infizierten Computers ein und starten Sie ihn neu. Dadurch wird das Betriebssystem Microsoft Windows XP SP2 mit dem Interface des Programms Bart PE gestartet.
   Das Programm Bart PE besitzt eine integrierte Netzwerkunterstützung für die Verwendung eines lokalen Netzwerks. Beim Start des Programms erfolgt auf dem Bildschirm eine Bestätigungsabfrage. Bestätigen Sie das Aktivieren der Netzwerkunterstützung, wenn Sie vor der Untersuchung des Computers planen, die Bedrohungssignaturen aus dem lokalen Netzwerk zu aktualisieren. Wenn kein Update erforderlich ist, lehnen Sie das Aktivieren der Netzwerkunterstützung ab.
3. Führen Sie den Befehl **GO→Programs→Kaspersky Internet Security 6.0→Start** aus, um Kaspersky Internet Security zu starten.

   Dadurch wird das Hauptfenster von Kaspersky Internet Security geöffnet. Im Notfall-Modus zur Systemwiederherstellung sind nur die Aufgaben zur Virensuche und (falls die Netzwerkunterstützung von Bart PE aktiviert ist) zum Update der Bedrohungssignaturen aus einem lokalen Netzwerk verfügbar.
4. Starten Sie die Virenuntersuchung des Computers.

Beachten Sie, dass für die Untersuchung standardmäßig die Bedrohungssignaturen verwendet werden, die am Erstellungsdatum der Notfall-CD aktuell waren. Aus diesem Grund wird empfohlen, die Datenbanken der

Bedrohungssignaturen vor Untersuchungsbeginn zu aktualisieren.

Außerdem ist zu beachten, dass die aktualisierten Datenbanken der Bedrohungssignaturen von der Anwendung nur in der laufenden Sitzung mit der Notfall-CD verwendet werden, d.h. bis zum Neustart des Computers.

Achtung!

Wenn bei der Untersuchung des Computers infizierte oder möglicherweise infizierte Objekte gefunden wurden, und diese aufgrund der Bearbeitung in die Quarantäne oder ins Backup verschoben wurden, wird empfohlen, die Bearbeitung dieser Objekte während der laufenden Sitzung mit der Notfall-CD abzuschließen.

Andernfalls gehen diese Objekte nach dem Neustart des Computers verloren.

17.11. Verwendung zusätzlicher Dienste

Kaspersky Internet Security bietet Ihnen an, folgende zusätzlichen Dienste zu verwenden:

- Benachrichtigung des Benutzers per E-Mail über das Eintreten bestimmter Ereignisse bei der Arbeit des Programms.
- Selbstschutz von Kaspersky Internet Security vor dem Beenden, Löschen und Verändern von Modulen, sowie Kennwortschutz für den Zugriff auf das Programm.
- Lösen von Kompatibilitätsproblemen mit Kaspersky Internet Security bei der Arbeit mit anderen Anwendungen.

Um zur Konfiguration der genannten Dienste zu gelangen,

1. Öffnen Sie das Konfigurationsfenster des Programms über den Link **Einstellungen** des Hauptfensters.
2. Wählen Sie den Punkt **Service** in der Konfigurationsstruktur.

Auf der rechten Seite können Sie festlegen, ob die Zusatzdienste bei der Programmarbeit verwendet werden sollen oder nicht.

17.11.1. Benachrichtigungen über die Ereignisse von Kaspersky Internet Security

Bei der Arbeit von Kaspersky Internet Security treten unterschiedliche Ereignisse ein. Sie können informativen Charakter besitzen oder wichtige Informationen enthalten. Ein Ereignis kann beispielsweise über die erfolgreiche Aktualisierung des Programms informieren oder einen Fehler bei der Arbeit einer bestimmten Komponente festhalten, der dringend behoben werden muss.

Um sich über die Ereignisse bei der Arbeit von Kaspersky Internet Security informieren zu lassen, können Sie den Dienst für Benachrichtigungen verwenden.

Die Benachrichtigungen können durch eine der folgenden Methoden erfolgen:

- Popup-Meldungen über dem Programmsymbol im Infobereich der Taskleiste
- Tonsignale
- E-Mail-Nachrichten
- Protokollieren von Informationen im Ereignisbericht

Um diesen Dienst zu verwenden,

1. Aktivieren Sie das Kontrollkästchen ☑ **Ereignisbenachrichtigung aktivieren** im Block **Interaktion mit dem Benutzer** (s. Abb. 105).

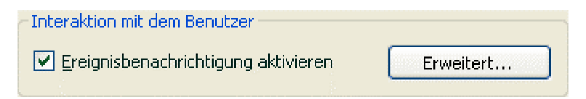


Abbildung 105. Aktivieren des Benachrichtigungsmodus

2. Legen Sie die Typen der Ereignisse von Kaspersky Internet Security fest, über deren Eintreten Sie benachrichtigt werden möchten, und wählen Sie eine Methode zum Senden der Benachrichtigungen (s. Pkt. 17.11.1.1 auf S. 300).
3. Passen Sie die Einstellungen für das Senden von Benachrichtigungen per E-Mail an, wenn Sie diese Benachrichtigungsmethode wünschen (s. Pkt. 17.11.1.2 auf S. 302).

17.11.1.1. Ereignistypen und Methoden zum Senden von Benachrichtigungen

Bei der Arbeit von Kaspersky Internet Security treten Ereignisse der folgenden Typen auf:

Kritische Ereignisse – Ereignisse mit kritischer Priorität. Es wird ausdrücklich empfohlen, sich über solche Ereignisse benachrichtigen zu lassen, weil sie auf Probleme bei der Arbeit des Programms oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Beispiele: *Die Bedrohungssignaturen sind beschädigt* oder *Die Lizenzgültigkeit ist abgelaufen*.

Funktionsstörung – Ereignisse, die zur Funktionsunfähigkeit der Anwendung führen. Beispielsweise das Fehlen einer Lizenz und der Bedrohungssignaturen.

Wichtige Ereignisse – Ereignisse, die unbedingt beachtet werden müssen, weil Sie wichtige Situationen bei der Programmarbeit wiedergeben. Beispiele: *Alle Schutzkomponenten sind deaktiviert* oder *Der Computer wurde lange nicht untersucht*.

Informative Ereignisse – Ereignisse mit informativem Charakter, die in der Regel keine wichtigen Informationen enthalten. Beispiele: *Alle gefährlichen Objekte wurden neutralisiert*.

Um festzulegen, über welche Ereignisse und auf welche Weise Sie benachrichtigt werden möchten:

1. Klicken Sie auf den Link Einstellungen im Programmhauptfenster.
2. Wählen Sie im Konfigurationsfenster des Programms den Abschnitt **Service**, aktivieren Sie das Kontrollkästchen ☑ **Ereignisbenachrichtigung aktivieren** und wechseln Sie mit der Schaltfläche **Erweitert** zu den ausführlichen Einstellungen.

Im folgenden Fenster **Benachrichtigungseinstellungen** (s. Abb. 106) können Sie folgende Benachrichtigungsmethoden für die oben genannten Ereignisse anpassen:

- *Popup-Meldung* über dem Programmsymbol im Infobereich. Die Meldung enthält Informationen über das eingetretene Ereignis.

  Um diesen Typ der Benachrichtigung zu verwenden, aktivieren Sie das Kontrollkästchen ☑ in der Spalte **Anzeige** gegenüber dem Ereignis, über das Sie benachrichtigt werden möchten.

- *Tonsignale.*

Wenn Sie möchten, dass die Benachrichtigung von einem Audiosignal begleitet wird, aktivieren Sie das Kontrollkästchen in der Spalte **Ton** neben dem Ereignis.

- *Benachrichtigung per E-Mail*.

  Um diesen Typ der Benachrichtigung zu verwenden, aktivieren Sie das Kontrollkästchen in der Spalte **E-Mail** gegenüber dem Ereignis, über das Sie benachrichtigt werden möchten, und passen Sie die Parameter für das Senden von Benachrichtigungen an (s. Pkt. 17.11.1.2 auf S. 302).

- *Protokollieren von Informationen im Ereignisbericht*.

  Damit Informationen über das Eintreten eines bestimmten Ereignisses im Bericht protokolliert werden, aktivieren Sie das Kontrollkästchen in der Spalte **Bericht** gegenüber dem Ereignis und passen Sie die Parameter für den Ereignisbericht an (s. Pkt. 17.11.1.3 auf S. 303.)

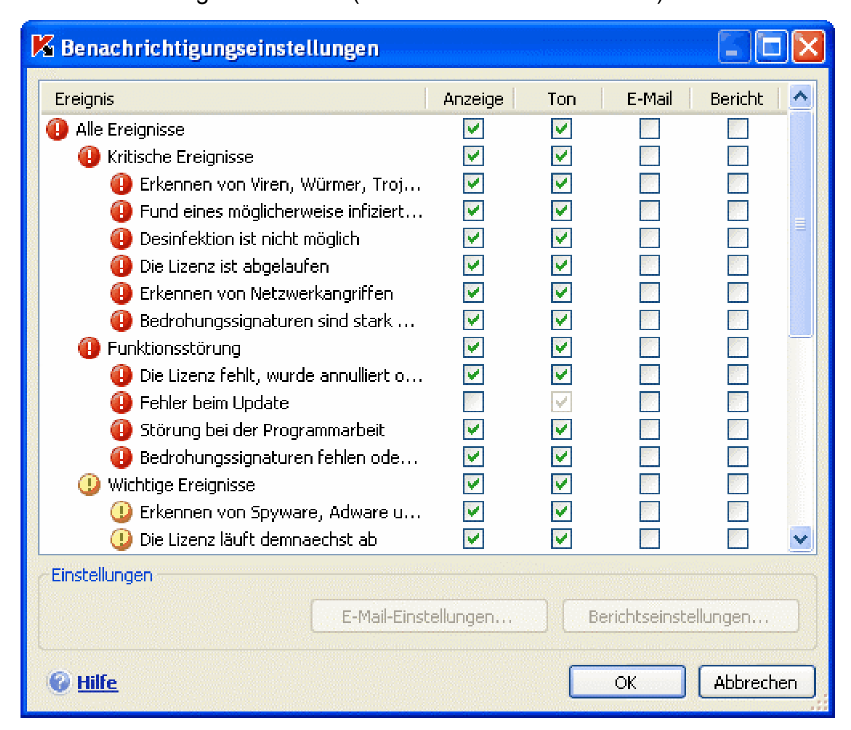


Abbildung 106. Ereignisse bei der Programmarbeit und entsprechende Benachrichtigungsmethoden

17.11.1.2. Konfiguration des Sendens von Benachrichtigungen per E-Mail

Nachdem Sie die Ereignisse gewählt haben (s. Pkt. 17.11.1.1 auf S. 300), über deren Eintreten Sie per E-Mail benachrichtigt werden möchten, müssen Sie die folgenden Einstellungen für das Senden der Benachrichtigungen vornehmen:

1. Öffnen Sie das Konfigurationsfenster des Programms über den Link **Einstellungen** des Hauptfensters.

2. Wählen Sie den Punkt **Service** in der Konfigurationsstruktur.

3. Klicken Sie im Block **Interaktion mit dem Benutzer** auf der rechten Seite des Fensters auf die Schaltfläche **Erweitert**.

4. Aktivieren Sie auf der Registerkarte **Benachrichtigungseinstellungen** (s. Abb. 106) in der Spalte **E-Mail** die Kontrollkästchen für die Ereignisse, bei deren Eintreten eine E-Mail-Benachrichtigung gesendet werden soll.

5. Legen Sie im Fenster (s. Abbildung 107), das mit der Schaltfläche **E-Mail-Einstellungen** geöffnet wird, folgende Parameter für das Senden von E-Mail-Benachrichtigungen fest:

   - Geben Sie im Block **Benachrichtigungsabsender** die Parameter des Absenders der Benachrichtigungen an.

   - Geben Sie im Block **Benachrichtigungsempfänger** die E-Mail-Adresse an, an welche die Benachrichtigungen geschickt werden sollen.

   - Geben Sie im Block **Versandmodus** den Modus zum Senden der Benachrichtigungen per E-Mail an. Damit das Programm die Nachricht beim tatsächlichen Eintreten eines Ereignisses abschickt, wählen Sie **Bei Ereigniseintritt**. Erstellen Sie zur Benachrichtigung über Ereignisse nach einem bestimmten Zeitraum einen Zeitplan für das Senden von Nachrichten. Klicken Sie dazu auf die Schaltfläche **Ändern**. Standardmäßig erfolgt die Benachrichtigung täglich.

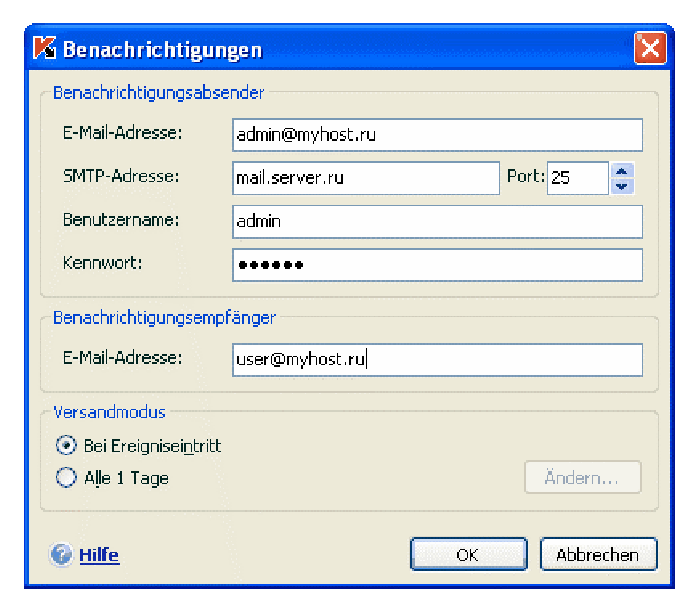


Abbildung 107. Einstellungen für E-Mail-Benachrichtigung

17.11.1.3. Parameter des Ereignisberichts

Um die Parameter des Ereignisberichts anzupassen:

1. Öffnen Sie im Hauptfenster mit dem Link Einstellungen das Konfigurationsfenster des Programms.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Service**.
3. Klicken Sie auf der rechten Seite des Fensters im Block **Interaktion mit dem Benutzer** auf die Schaltfläche **Erweitert**.

Wählen Sie im Fenster **Benachrichtigungseinstellungen** für das gewünschte Ereignis die Option zur Protokollierung im Bericht und klicken Sie auf die Schaltfläche **Berichtseinstellungen**.

Kaspersky Internet Security bietet die Möglichkeit, Informationen über Ereignisse, die bei der Arbeit der Anwendung eintreten, im allgemeinen Ereignisbericht von Microsoft Windows (**Anwendung**) oder in einem separaten Ereignisbericht von Kaspersky Internet Security (**Kaspersky Event Log**) aufzuzeichnen.

Auf einem Computer mit dem Betriebssystem Microsoft Windows 98/ME ist das Führen von Ereignisberichten nicht möglich. Unter dem Betriebssystem Microsoft Windows NT 4.0 steht der Bericht **Kaspersky Event Log** nicht zur Verfügung.

Diese Einschränkungen hängen mit Besonderheiten der genannten Betriebssysteme zusammen.

Zur Anzeige der Berichte dient das Microsoft Windows-Standardfenster **Ereignisanzeige**, das mit Hilfe des folgenden Befehls geöffnet wird: **Start** → **Einstellungen** → **Systemsteuerung** → **Verwaltung** → **Ereignisanzeige**.

17.11.2. Selbstschutz und Zugriffs-beschränkung für das Programm

Kaspersky Internet Security ist ein Programm, das den Computer vor schädlichen Programmen schützt, und wird dadurch selbst zu einem Ziel für schädliche Programme, die versuchen, die Arbeit des Programms zu blockieren oder es sogar vom Computer zu löschen.

Außerdem kann ein PC von verschiedenen Benutzern verwendet werden, deren Fertigkeiten im Umgang mit Computern möglicherweise nicht ausreichend sind. Der ungehinderte Zugriff auf das Programm und dessen Einstellungen kann das Sicherheitsniveau des Computers stark einschränken.

Um die Stabilität des Sicherheitssystems Ihres Computers zu gewährleisten, verfügt das Programm über Mechanismen zum Selbstschutz, zum Schutz vor externem Zugriff und zum Kennwortschutz für den Programmzugriff.

Wenn Kaspersky Internet Security auf einem Computer mit dem Betriebssystem Microsoft Windows 98/ME installiert ist, steht der Dienst zum Selbstschutz der Anwendung nicht zur Verfügung.

Für 64-Bit-Betriebssysteme und für Microsoft Windows Vista steht der Selbstschutzmechanismus der Anwendung nur im Hinblick auf Veränderungen oder das Löschen von Dateien auf der Festplatte sowie von Einträgen in der Systemregistrierung zur Verfügung.

Um die Selbstschutzmechanismen für das Programm zu aktivieren:

1. Öffnen Sie das Konfigurationsfenster des Programms mit dem Link Einstellungen des Hauptfensters.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Service**.
3. Nehmen Sie im Block **Selbstschutz** (s. Abb. 108) die entsprechenden Einstellungen vor:

☑ **Selbstschutz aktivieren**. Wenn dieses Kontrollkästchen aktiviert ist, wird der Mechanismus zum Schutz des Programms vor dem Verändern oder Löschen von eigenen Dateien auf der Festplatte, Prozessen im Arbeitsspeicher und Einträgen in der Systemregistrierung wirksam.

☑ **Externe Dienststeuerung verbieten**. Wenn dieses Kontrollkästchen aktiviert ist, wird jeder Versuch zur Fernsteuerung von Diensten der Anwendung blockiert.

Wird versucht, eine der oben genannten Aktionen auszuführen, dann erscheint eine Meldung über dem Programmsymbol im Infobereich der Taskleiste (falls der Benachrichtigungsdienst nicht vom Benutzer deaktiviert wurde).



Abbildung 108. Einstellungen für den Programmschutz

Um den Zugriff auf das Programm mit Hilfe eines Kennworts zu schützen, aktivieren Sie das Kontrollkästchen ☑ **Kennwortschutz aktivieren** und geben Sie im Fenster, das mit der Schaltfläche **Einstellungen** geöffnet wird, das Kennwort und den Bereich an, für den die Zugriffsbeschränkung gelten soll (s. Abb. 109). Sie können entweder alle Operationen mit dem Programm blockieren (unter Ausnahme der Arbeit mit Meldungen über den Fund gefährlicher Objekte) oder das Ausführen folgender Aktionen untersagen:

- Die Einstellungen für die Arbeit des Programms ändern.
- Die Arbeit von Kaspersky Internet Security beenden.
- Den Schutz Ihres Computers deaktivieren oder vorübergehend anhalten.

Jede der oben genannten Aktionen führt zu einer Verringerung des Schutzniveaus Ihres Computers. Deshalb sollten Sie festlegen, welche Benutzer Ihres Computers berechtigt sein sollen, diese Aktionen auszuführen.

Beim Versuch eines beliebigen Benutzers Ihres Computers, die von Ihnen festgelegten Aktionen auszuführen, wird das Programm nun immer das Kennwort abfragen.

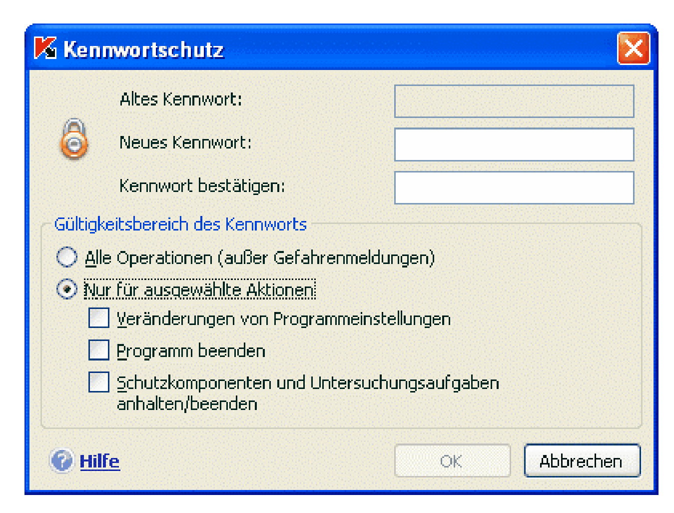


Abbildung 109. Einstellungen für den Kennwortschutz des Programms

17.11.3. Lösen von Kompatibilitätsproblemen von Kaspersky Internet Security mit anderen Anwendungen

In einigen Fällen können bei der Verwendung von Kaspersky Internet Security Konflikte bei der Arbeit mit Anwendungen, die auf dem Computer installiert sind, auftreten. Das steht mit dem in diese Programme integrierten Selbstschutzmechanismus in Verbindung, der reagiert, wenn Kaspersky Internet Security versucht, auf die Programme zuzugreifen. Zu diesen Programmen gehören beispielsweise das Plugin Authentica des Programms Adobe Reader, das der Zugriffskontrolle für Dokumente im pdf-Format dient, das Programm zur Steuerung von Mobiltelefonen Oxygen Phone Manager II, sowie einige Arten von Spielen, die über einen Crackschutz verfügen.

Um dieses Problem zu lösen, aktivieren Sie das Kontrollkästchen ☑ **Kompatibilität mit dem Selbstschutz von Anwendungen** im Abschnitt **Service** des Konfigurationsfensters der Anwendung. Damit die Änderungen dieses Parameters wirksam werden, ist der Neustart des Betriebssystems erforderlich.

Beachten Sie aber, dass ein Teil der Funktionalität von Kaspersky Internet Security (Untersuchung von VBA-Makros, Anti-Dialer) nicht verfügbar sein wird, wenn dieses Kontrollkästchen aktiviert ist. Wird eine dieser Komponenten

aktiviert, dann wird der Kompatibilitätsmodus im Selbstschutz für Anwendungen automatisch ausgeschaltet. Nachdem diese Komponenten aktiviert wurden, beginnen sie erst nach dem Neustart der Anwendung zu arbeiten.

17.12. Export/Import der Einstellungen von Kaspersky Internet Security

Kaspersky Internet Security bietet Ihnen die Möglichkeit zum Exportieren und Importieren der Programmeinstellungen.

Diese Option kann beispielsweise von Nutzen sein, wenn Sie das Programm auf Ihrem Privat-PC und im Büro installiert haben. Sie können das Programm zu Hause entsprechend konfigurieren, die Einstellungen auf einer Diskette speichern und mit Hilfe der Importfunktion schnell auf Ihren Computer im Büro laden. Die Einstellungen werden in einer speziellen Konfigurationsdatei gespeichert.

Um die aktuellen Programmeinstellungen zu exportieren,

1. Öffnen Sie das Hauptfenster von Kaspersky Internet Security.
2. Wählen Sie den Abschnitt **Service** und klicken Sie auf den Link Einstellungen.
3. Klicken Sie im Block **Konfigurationsverwaltung** auf die Schaltfläche **Speichern**.
4. Geben Sie Name und Pfad der Konfigurationsdatei an.

Um die Programmeinstellungen aus einer Konfigurationsdatei zu importieren,

1. Öffnen Sie das Hauptfenster von Kaspersky Internet Security.
2. Wählen Sie den Abschnitt **Service** und klicken Sie auf den Link Einstellungen.
3. Klicken Sie auf die Schaltfläche **Laden** und wählen Sie die Datei, aus der Sie die Parameter für Kaspersky Internet Security importieren möchten.

17.13. Wiederherstellen der Standardeinstellungen

Sie können jederzeit zu den empfohlenen Programmeinstellungen zurückkehren. Diese gelten als optimal und werden von den Kaspersky-Lab-Spezialisten empfohlen. Die Wiederherstellung der Einstellungen erfolgt mit Hilfe des Konfigurationsassistenten.

Um die Schutzeinstellungen wiederherzustellen,

1. Wählen Sie den Abschnitt **Service** und wechseln sie mit dem Link Einstellungen in das Konfigurationsfenster des Programms.
2. Klicken Sie im Abschnitt **Konfigurationsverwaltung** auf die Schaltfläche **Wiederherstellen**.

Im folgenden Fenster können Sie angeben, welche Parameter bei der Wiederherstellung der empfohlenen Sicherheitsstufe beibehalten werden und für welche Komponenten diese gelten sollen.

Die Liste enthält die Programmkomponenten, deren Parameter vom Benutzer verändert wurden oder vom Programm aufgrund des Trainings (Anti-Hacker und Anti-Spam) gesammelt wurden. Wenn für eine bestimmte Komponente bei der Arbeit exklusive Parameter festgelegt wurden, werden diese ebenfalls in der Liste angegeben.

Zu den exklusiven Parametern zählen die weißen und schwarzen Wörter- und Adressenlisten für Anti-Spam; die von Web-Anti-Virus und Anti-Spy verwendeten Listen der vertrauenswürdigen Internetadressen und Telefonnummern von Internetprovidern; die für die Schutzkomponenten erstellten Ausnahmeregeln; Anti-Hacker-Filterregeln für Pakete und Anwendungen sowie Regeln für Anwendungen für den Proaktiven Schutz.

Diese Listen werden während der Arbeit des Programms erstellt. Da ihnen individuelle Aufgaben und Sicherheitsanforderungen zugrunde liegen, kann das Erstellen dieser Listen sehr zeitaufwändig sein. Deshalb wird empfohlen, sie beim Wiederherstellen der ursprünglichen Programmeinstellungen beizubehalten.

In der Grundeinstellung werden alle in der Liste enthaltenen Parameter gespeichert (die entsprechenden Kontrollkästchen sind deaktiviert). Wenn bestimmte Parameter nicht beibehalten werden sollen, entfernen Sie die entsprechenden Kontrollkästchen.

Klicken Sie zum Abschluss der Konfiguration auf die Schaltfläche **Weiter**. Der Konfigurationsassistent wird gestartet. Folgen Sie den Anweisungen.

Nach dem Abschluss des Assistenten wird für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** eingestellt, wobei die von Ihnen zum Speichern gewählten Parameter berücksichtigt werden. Zusätzlich werden die Einstellungen übernommen, die Sie während der Arbeit des Assistenten vorgenommen haben.

KAPITEL 18. ARBEIT MIT DEM PROGRAMM AUS DER BEFEHLSZEILE

Sie können mit Kaspersky Internet Security mit Hilfe der Befehlszeile arbeiten. Dabei ist die Möglichkeit zum Ausführen der folgenden Operationen vorgesehen:

- Starten, Beenden, Anhalten und Fortsetzen der Arbeit von Komponenten der Anwendung.
- Starten, Beenden, Anhalten und Fortsetzen der Arbeit von Aufgaben zur Virensuche.
- Erhalt von Informationen über den aktuellen Status von Komponenten und Aufgaben sowie ihrer Statistik.
- Untersuchung von ausgewählten Objekten.
- Update der Bedrohungssignaturen und Programm-Module.
- Aufruf der Hilfe über die Syntax der Befehlszeile.
- Aufruf der Hilfe über die Syntax eines Befehls.

Syntax der Befehlszeile:

```
avp.com <Befehl> [Parameter]
```

Als **<Befehl>** werden verwendet:

ACTIVATE	Aktivierung der Anwendung über das Internet mit Hilfe eines Aktivierungscodes
ADDKEY	Aktivierung der Anwendung mit Hilfe einer Lizenzschlüsseldatei
START	Starten einer Komponente oder Aufgabe
PAUSE	Anhalten der Arbeit einer Komponente oder Aufgabe
RESUME	Fortsetzen der Arbeit einer Komponente oder Aufgabe
STOP	Beenden der Arbeit einer Komponente oder Aufgabe

STATUS	Bildschirmanzeige des aktuellen Status einer Komponente oder Aufgabe
STATISTICS	Bildschirmanzeige der Statistik über die Arbeit einer Komponente oder Aufgabe
HELP	Hilfe über die Befehlssyntax, Anzeige einer Befehlsliste
SCAN	Untersuchung von Objekten auf das Vorhandensein von Viren
UPDATE	Starten des Programmupdates
ROLLBACK	Rückgängigmachen des letzten Updates der Anwendung
EXIT	Beenden der Arbeit mit dem Programm (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
IMPORT	Importieren von Schutzeinstellungen für Kaspersky Internet Security
EXPORT	Exportieren von Schutzeinstellungen für Kaspersky Internet Security

Jedem Befehl entspricht eine eigene Auswahl von Parametern, die für eine konkrete Komponente von Kaspersky Internet Security spezifisch sind.

18.1. Aktivierung der Anwendung

Die Aktivierung der Anwendung kann auf zwei Arten erfolgen:

- über das Internet mit Hilfe eines Aktivierungscodes (Befehl ACTIVATE)
- mit Hilfe einer Lizenzschlüsseldatei (Befehl ADDKEY)

Syntax der Befehlszeile:

```
ACTIVATE <Aktivierungscode>
```

```
ADDKEY <Dateiname>
```

Beschreibung der Parameter:

<Aktivierungscode>	Aktivierungscode für die Anwendung, den Sie beim Erwerb des Produkts erhalten haben.
<Dateiname>	Name der Lizenzschlüsseldatei für die Anwendung (Endung **.key*).

Beispiel:

```
avp.com ACTIVATE 00000000-0000-0000-0000-000000000000
avp.com ADDKEY 00000000.key
```

18.2. Steuerung von Anwendungskomponenten und Aufgaben

Die Steuerung der Komponenten und Aufgaben von Kaspersky Internet Security wird mit Hilfe der folgenden Befehle ausgeführt:

- START
- PAUSE
- RESUME
- STOP
- STATUS
- STATISTICS

Die Aufgabe oder Komponente, auf die der Befehl angewandt wird, wird durch die Parameter des Befehls bestimmt.

> Die Befehle STOP und PAUSE werden nur ausgeführt, wenn das über die Programmoberfläche festgelegte Kennwort für Kaspersky Internet Security angegeben wird.

Syntax der Befehlszeile:

```
avp.com <Befehl> <profile|taskid>
avp.com STOP
```

```
PAUSE <profile|taskid> /password=<Kennwort>
```

Für den Parameter **<profile|taskid>** wird einer der folgenden Werte angegeben:

RTP	alle Schutzkomponenten
FM	Datei-Anti-Virus
EM	Mail-Anti-Virus
WM	Web-Anti-Virus
BM	Proaktiver Schutz
ASPY	Anti-Spy
AH	Anti-Hacker
AS	Anti-Spam
UPDATER	Update
SCAN_OBJECTS	die Aufgabe "*Virensuche*"
SCAN_MY_COMPUTER	die Aufgabe "Arbeitsplatz"
SCAN_CRITICAL_AREAS	die Aufgabe *"Kritische Bereiche"*
SCAN_STARTUP	die Aufgabe "Autostart-Objekte"
<Aufgabenname>	benutzerdefinierte Aufgabe

Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die im Interface des Programms festgelegt wurden.

Beispiele:

Um Datei-Anti-Virus zu aktivieren, geben Sie in der Befehlszeile ein:

```
avp.com START FM
```

Um den aktuellen Status des Proaktiven Schutzes für Ihren Computer anzuzeigen, geben Sie in der Befehlszeile ein:

```
avp.com STATUS BM
```

Um die Aufgabe Arbeitsplatz zu beenden, geben Sie in der Befehlszeile ein:

```
avp.com STOP SCAN_MY_COMPUTER /password=<Kennwort>
```

18.3. Virenuntersuchung von Objekten

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zur Bearbeitung von schädlichen Objekten besitzt folgendes allgemeines Aussehen:

```
avp.com SCAN [<Untersuchungsobjekt>] [<Aktion>]
[<Aktionsanfrage>] [<Dateitypen>] [<Ausnahmen>]
[<Konfigurationsdatei>] [<Berichtsparameter>]
```

> Für die Untersuchung von Objekten können Sie auch die in Kaspersky Internet Security erstellten Aufgaben verwenden, indem Sie die erforderliche Befehlszeile benutzen (s. Pkt. 18.1 auf S. 311). Dabei wird die Aufgabe mit den Parametern ausgeführt, die im Interface des Produkts festgelegt wurden.

Beschreibung der Parameter.

<table>
<tr><td colspan="2"><Untersuchungsobjekt> - Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen.

Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.</td></tr>
<tr><td><files></td><td>Liste mit den Pfaden der Dateien und/oder Ordner für die Untersuchung.

Die Angabe des absoluten oder relativen Pfads ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen.

Kommentare:

a. Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt.

b. Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.</td></tr>
</table>

/MEMORY	Objekte des Arbeitsspeichers.
/STARTUP	Autostart-Objekte.
/MAIL	Maildatenbanken.
/REMDRIVES	alle Wechseldatenträger.
/FIXDRIVES	alle lokalen Laufwerke.
/NETDRIVES	alle Netzwerklaufwerke.
/QUARANTINE	Objekte in Quarantäne.
/ALL	vollständige Untersuchung des Computers.
/@:<filelist.lst>	Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Die Datei muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Pfad ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt.
<Aktion> - Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **/i2** entspricht.	
/i0	Keine Aktion ausführen, nur Informationen im Bericht protokollieren.
/i1	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen.
/i2	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen (diese Aktion wird standardmäßig verwendet).

/i3	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i4	infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
<Aktionsanfrage> - Der Parameter bestimmt für welche Aktionen während der Untersuchung eine Bestätigungsabfrage an den Benutzer erfolgt. Wenn der Parameter nicht angegeben wird, wird die Aktion standardmäßig am Ende der Untersuchung erfragt.	
/i8	den Benutzer beim Fund eines infizierten Objekts nach einer Aktion fragen
/i9	den Benutzer nach dem Abschluss der Untersuchung nach einer Aktion fragen
<Dateitypen> - Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht.	
/fe	nur infizierbare Dateien nach Erweiterung untersuchen.
/fi	nur infizierbare Dateien nach Inhalt untersuchen.
/fa	Alle Dateien untersuchen.
<Ausnahmen> - Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
/e:a	Archive nicht untersuchen.
/e:b	Maildatenbanken nicht untersuchen.
/e:m	E-Mail-Nachrichten im Format plain text nicht untersuchen.

/e:<mask>	Objekte nach Maske nicht untersuchen.
/e:<seconds>	Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter <seconds> angegebene Zeitraum.
/es:<size>	Objekte überspringen, deren Größe (in MB) über dem Wert liegt, der durch den Parameter **<size>** bestimmt wird.
<Konfigurationsdatei> - bestimmt den Pfad der Konfigurationsfenster, in der die Parameter für die Arbeit des Programms bei der Untersuchung enthalten sind. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die im Interface von Kaspersky Internet Security festgelegt wurden.	
/C:<settings_file>	Die Werte der Parameter, die in der Datei **<settings_file>** angegeben sind, verwenden.
<Berichtsparameter> - Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt. Alle Ereignisse werden angezeigt.	
/R:<report_file>	nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
/RA:<report_file>	alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren.

Beispiele:

Untersuchung des Arbeitsspeichers, der Autostart-Objekte, der Maildatenbanken sowie der Ordner **My Documents**, **Program Files** *und der Datei* **test.exe***:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Anhalten der Untersuchung von ausgewählten Objekten, Starten der vollständigen Untersuchung des Computers, bei Abschluss der Untersuchung

soll die Virensuche in den ausgewählten Objekten fortgesetzt werden:

```
avp.com PAUSE SCAN_OBJECTS /password=<Kennwort>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Untersuchung der Objekte, deren Liste in der Datei **object2scan.txt** angegeben ist. Für die Arbeit soll die Konfigurationsdatei **scan_setting.txt** verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

18.4. Programmupdate

Der Befehl für das Update der Programm-Module und Bedrohungssignaturen von Kaspersky Internet Security besitzt folgende Syntax:

```
avp.com UPDATE [<path/URL>] [/R[A]:<report_file>]
[/C:<settings_file>] [/APP]
```

Beschreibung der Parameter:

[<path/URL>]	HTTP-, FTP-Server oder Netzwerkordner für den Download der Updates. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Einstellungen des Diensts für das Programmupdate übernommen.
/R[A]:<report_file>	**/R:<report_file>** - nur wichtige Ereignisse im Bericht protokollieren. **/R[A]:<report_file>** - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt. Alle Ereignisse werden angezeigt.

/C:<settings_file>	Pfad der Konfigurationsdatei, die die Parameter für die Arbeit des Programms beim Update enthält. Die Angabe des absoluten oder relativen Pfads ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die im Interface von Kaspersky Internet Security festgelegt wurden.
/APP	Programm-Module aktualisieren.

Beispiele:

Update der Bedrohungssignaturen, alle Ereignisse protokollieren:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Update der Programm-Module von Kaspersky Internet Security, die Parameter der Konfigurationsdatei **updateapp.ini** verwenden:*

```
avp.com UPDATE /APP /C:updateapp.ini
```

18.5. Rückgängigmachen des letzten Updates der Anwendung

Syntax der Befehlszeile:

```
ROLLBACK [/R[A]:<report_file>]
```

/R[A]:<report_file>	**/R:<report_file>** - nur wichtige Ereignisse im Bericht festhalten. **/R[A]:<report_file>** - alle Ereignisse im Bericht festhalten. Es kann der absolute oder relative Pfad der Datei angegeben werden. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Beispiel:

```
avp.com ROLLBACK /RA:rollback.txt
```

18.6. Export von Schutzparametern

Syntax der Befehlszeile:

```
avp.com EXPORT <profile|taskid> <Dateiname>
```

Beschreibung der Parameter:

<profile>	Komponente oder Aufgabe, für die der Export von Parametern ausgeführt wird. Einer der folgenden Werte kann verwendet werden: **RTP** - alle Schutzkomponenten **FM** - Datei-Anti-Virus **EM** - Mail-Anti-Virus **WM** - Web-Anti-Virus **BM** - Proaktiver Schutz **ASPY** – Anti-Spy **AH** - Anti-Hacker **AS** - Anti-Spam
<Dateiname>	Pfad der Datei, in welche die Parameter von Kaspersky Internet Security exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden. Die Konfigurationsdatei wird im Binärformat (dat) gespeichert und kann später zum Übertragen von Anwendungseinstellungen auf andere Computer verwendet werden. Die Konfigurationsdatei kann auch im Textformat gespeichert werden. Dazu erhält der Dateiname die Endung *txt*.

Beispiele:

```
avp.com EXPORT c:\settings.dat
```

18.7. Import von Schutzparametern

Syntax der Befehlszeile:

```
avp.com IMPORT <Dateiname> [/password=<Kennwort>]
```

<Dateiname>	Pfad der Datei, aus welcher die Parameter von Kaspersky Internet Security importiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.
<Kennwort>	Kennwort für Kaspersky Internet Security, das auf der Anwendungsoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.

Beispiel:

```
avp.com IMPORT c:\settings.dat /password=<Kennwort>
```

18.8. Anwendung starten

Syntax der Befehlszeile:

```
avp.com
```

18.9. Anwendung beenden

Syntax der Befehlszeile:

```
EXIT /password=<Kennwort>
```

<Kennwort>	Kennwort für Kaspersky Internet Security, das auf der Anwendungsoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.

18.10. Anzeige der Hilfe

Zur Anzeige der Hilfe über die Syntax der Befehlzeile dient folgender Befehl:

```
avp.com [ /? | HELP ]
```

Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
avp.com <Befehl> /?
avp.com HELP <Befehl>
```

18.11. Rückgabecodes der Befehlszeile

In diesem Abschnitt werden die Rückgabecodes der Befehlszeile beschrieben. Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Als Rückgabecodes für Aufgaben sind die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp möglich.

Allgemeine Rückgabecodes	
0	Operation wurde erfolgreich ausgeführt
1	Ungültiger Parameterwert
2	Unbekannter Fehler
3	Fehler bei der Aufgabenausführung
4	Aufgabenausführung wurde abgebrochen
Rückgabecodes für Aufgaben zur Virensuche	
101	Alle gefährlichen Objekte wurden bearbeitet
102	Es wurden gefährliche Objekte gefunden

KAPITEL 19. PROGRAMM ÄNDERN, REPARIEREN ODER LÖSCHEN

Das Programm kann auf zwei Arten deinstalliert werden:

- mit Hilfe des Installationsassistenten der Anwendung (s. Pkt. 19.1 auf S. 323);
- aus der Befehlszeile (s. Pkt. 19.2 auf S. 326).

19.1. Ändern, Reparieren oder Löschen des Programms mit Hilfe des Installationsassistenten

Die Reparatur des Programms kann dann von Nutzen sein, wenn Sie Fehler in seiner Arbeit feststellen, die auf inkorrekte Einstellungen oder beschädigte Programmdateien zurückgehen.

Das Ändern des Komponentenbestands erlaubt Ihnen, bestimmte Komponenten von Kaspersky Internet Security nachträglich zu installieren oder jene Komponenten zu löschen, die Sie bei der Arbeit stören oder nicht gebraucht werden.

Um den ursprünglichen Programmzustand wiederherzustellen, um Komponenten von Kaspersky Internet Security, die bei der Erstinstallation nicht installiert wurden, zu installieren, oder um das Programm zu löschen,

1. Löschen Sie das Programm aus dem Arbeitsspeicher. Klicken Sie dazu mit der rechten Maustaste auf das Programmsymbol in der Taskleiste und wählen Sie im folgenden Kontextmenü den Punkt **Beenden**.
2. Legen Sie die CD mit der Programmdistribution in das CD-ROM-Laufwerk ein, wenn die Installation von dort aus erfolgte. Wenn die Installation von Kaspersky Internet Security aus einer anderen Quelle erfolgte (gemeinsamer Ordner, Ordner auf der Festplatte usw.),

vergewissern Sie sich, dass die Programmdistribution in diesem Ordner vorhanden ist und Sie zugriffsberechtigt sind.

3. Wählen Sie **Start** → **Programme** → **Kaspersky Internet Security 6.0** → **Ändern, Reparieren oder Löschen**.

Dadurch wird das Installationsprogramm in Form eines Assistenten gestartet. Im Folgenden werden die Schritte zur Reparatur, zum Ändern des Bestands der Programmkomponenten und zum Löschen des Programms ausführlich beschrieben.

Schritt 1. Startfenster des Installationsprogramms

Wenn Sie alle oben beschriebenen Aktionen ausgeführt haben, die für die Reparatur oder das Ändern des Komponentenbestands erforderlich sind, wird auf dem Bildschirm das Begrüßungsfenster des Installationsprogramms für Kaspersky Internet Security geöffnet. Klicken Sie auf die Schaltfläche **Weiter**.

Schritt 2. Auswahl einer Operation

Nun müssen Sie festlegen, welche Operation Sie mit dem Programm vornehmen möchten: Zur Auswahl stehen das Ändern der Programmkomponenten, das Wiederherstellen des ursprünglichen Zustands der installierten Komponenten oder das Löschen bestimmter Komponenten oder des ganzen Programms. Klicken Sie zum Ausführen der von Ihnen gewünschten Operation auf die entsprechende Schaltfläche. Die weitere Aktion des Installationsprogramms ist von der gewählten Operation abhängig.

Das Ändern des Komponentenbestands entspricht der benutzerdefinierten Installation des Programms (s. Schritt 6 auf S. 36), bei der Sie festlegen können, welche Komponenten installiert und welche gelöscht werden sollen.

Die Reparatur des Programms erfolgt auf Basis der installierten Komponenten. Alle Dateien der Komponenten, die installiert sind, werden aktualisiert und für jede dieser Komponenten wird die empfohlene Sicherheitsstufe eingestellt.

Beim Löschen des Programms können Sie wählen, welche der bei der Arbeit des Programms erstellten und verwendeten Daten, auf Ihrem Computer gespeichert werden sollen. Um alle Daten von Kaspersky Internet Security zu löschen, wählen Sie die Variante **Die Anwendung vollständig löschen**. Um bestimmte Daten zu speichern, wählen Sie die Variante **Objekte der Anwendung speichern** und geben Sie an, welche Objekte beibehalten werden sollen:

- *Aktivierungsdaten* – Lizenzschlüssel oder Aktivierungscode des Programms

- *Bedrohungssignaturen* – vollständige Signaturen der gefährlichen Programme, Viren und anderen Bedrohungen, die beim letzten Update aktuell waren.
- *Anti-Spam-Wissensdatenbank* – Wissensdatenbank, auf deren Basis unerwünschte E-Mails erkannt werden können. Diese Datenbank enthält detaillierte Informationen darüber, welche Mails für Sie als Spam gelten und welche als nützlich.
- *Backup-Objekte* – Sicherungskopien von gelöschten oder desinfizierten Objekten. Es wird empfohlen, diese Objekte zu speichern, um sie bei Bedarf später wiederherzustellen.
- *Quarantäneobjekte* – Objekte, die möglicherweise von Viren oder Virusmodifikationen infiziert sind. Solche Objekte enthalten Code, der Ähnlichkeit mit dem Code eines bekannten Virus besitzt. Allerdings lässt sich nicht sicher sagen, ob sie schädlich sind. Es wird empfohlen, diese Objekte zu speichern, weil sie sich als virusfrei erweisen oder später unter Verwendung von aktualisierten Bedrohungssignaturen desinfiziert werden können.
- *Schutzeinstellungen* – Parameterwerte für die Arbeit aller Programmkomponenten.
- *iSwift-Daten* – Datenbank, die Informationen über untersuchte Objekte des NTFS-Dateisystems enthält. Sie erlaubt die Beschleunigung der Untersuchung von Objekten. Durch die Verwendung dieser Datenbank untersucht Kaspersky Internet Security nur jene Objekte, die seit der letzten Untersuchung verändert wurden.

> Achtung.
>
> Wenn zwischen der Deinstallation einer Version von Kaspersky Internet Security und der Installation einer anderen Version ein größerer Zeitraum liegt, wird davon abgeraten, die aus der vorherigen Programminstallation stammende *iSwift*-Datenbank zu verwenden. In der Zwischenzeit kann ein gefährliches Programm auf den Computer gelangt sein, dessen schädliche Aktionen bei Verwendung dieser Datenbank nicht erkannt werden, was zu einer Infektion des Computers führen kann.

Klicken Sie auf die Schaltfläche **Weiter**, um die gewählte Operation zu starten. Der Prozess zum Kopieren der notwendigen Dateien auf Ihren Computer oder zum Löschen der ausgewählten Komponenten und Daten wird gestartet.

Schritt 3. Abschluss der Operation zum Reparieren, Ändern oder Löschen des Programms

Der Prozess zum Reparieren, Ändern oder Löschen wird auf dem Bildschirm dargestellt. Danach werden Sie über den Abschluss der Operation informiert.

Die Deinstallation macht in der Regel den Neustart des Computers erforderlich, weil Änderungen im System berücksichtigt werden müssen. Auf dem Bildschirm erscheint eine Bestätigungsabfrage für den Neustart des Computers. Klicken Sie auf die Schaltfläche **Ja**, um den Neustart sofort vorzunehmen, oder auf die Schaltfläche **Nein**, um den Computer später manuell neu zu starten.

19.2. Deinstallation des Programms aus der Befehlszeile

Um Kaspersky Internet Security aus der Befehlszeile zu deinstallieren, geben Sie ein:

```
msiexec /x <Paketname>
```

Es wird ein Installationsassistent gestartet (s. Kapitel 19 auf S. 323), mit dessen Hilfe Sie die Deinstallation der Anwendung vornehmen können.

Außerdem können Sie zur Deinstallation der Anwendung eine der folgenden Methoden verwenden.

Um die Anwendung im Silent-Modus ohne Neustart des Computers zu deinstallieren (der Neustart muss nach der Deinstallation manuell erfolgen), geben Sie folgende Befehlszeile ein:

```
msiexec /x <Paketname> /qn
```

Um die Anwendung im Silent-Modus mit anschließendem Neustart des Computers zu deinstallieren, geben Sie folgende Befehlszeile ein:

```
msiexec /x <Paketname> ALLOWREBOOT=1 /qn
```

KAPITEL 20. HÄUFIGE FRAGEN

In diesem Kapitel behandeln wir die von Benutzern am häufigsten gestellten Fragen zu Installation, Konfiguration und Arbeit mit Kaspersky Internet Security und versuchen, sie eingehend zu beantworten.

Frage: *Kann Kaspersky Internet Security 6.0 mit Antivirenprodukten anderer Hersteller genutzt werden?*

Um Konflikte zu vermeiden, empfehlen wir, die Antiviren-Software anderer Hersteller vor der Installation von Kaspersky Internet Security zu deinstallieren.

Frage: *Eine Datei wird von Kaspersky Internet Security nicht wiederholt untersucht. Warum?*

In der Tat untersucht Kaspersky Internet Security eine Datei nicht doppelt, wenn sie seit der letzten Untersuchung nicht geändert worden ist.

Das wird durch die Verwendung der neuen Technologien iChecker™ und iSwift™ ermöglicht. Dabei eine Datenbank mit Kontrollsummen der Objekte verwendet und die Kontrollsummen von Dateien werden in zusätzlichen NTFS-Strömen gespeichert.

Frage: *Wozu wird der Lizenzschlüssel gebraucht? Funktioniert mein Kaspersky Internet Security auch ohne Lizenzschlüssel?*

Kaspersky Internet Security kann ohne Lizenzschlüssel arbeiten. Allerdings stehen in diesem Fall das Programmupdate und die Unterstützung durch den Technischen Support-Service nicht zur Verfügung.

Wenn Sie sich noch nicht für den Kauf von Kaspersky Internet Security entschieden haben, können wir Ihnen einen Testschlüssel mit einer Gültigkeit von zwei Wochen oder einen Monat anbieten. Nach Ablauf der Testdauer wird der Schlüssel gesperrt.

Frage: *Nach der Installation von Kaspersky Internet Security verhält sich das Betriebssystem ungewöhnlich ("Einfrieren auf blauem Bildschirm", wiederholter Neustart des Computers u.a.). Was tun?*

Diese Situation tritt selten ein, kann aber durch einen Konflikt zwischen Kaspersky Internet Security und einem auf Ihrem Computer installierten Programm verursacht werden.

Gehen Sie folgendermaßen vor, um die Funktionsfähigkeit Ihres Betriebssystems wiederherzustellen:

1. Klicken Sie gleich nachdem der Computer gestartet wurde solange auf die Taste **F8**, bis das Auswahlmenü für die Startvarianten des Betriebssystems erscheint.
2. Wählen Sie den Punkt **Abgesicherter Modus** und laden Sie das Betriebssystem.
3. Starten Sie Kaspersky Internet Security.
4. Verwenden Sie im Programmhauptfenster den Link Einstellungen und wählen Sie im Konfigurationsfenster des Programms den Abschnitt **Schutz**.
5. Deaktivieren Sie das Kontrollkästchen **Programm beim Hochfahren des Computers starten** und klicken Sie auf die Schaltfläche **OK**.
6. Starten Sie das Betriebssystem im gewöhnlichen Modus neu.

Wenden Sie sich danach über die Kaspersky-Lab-Webseite an den Technischen Support-Service (Abschnitt **Dienste → Technischer Support → Anfrage an den Support senden**). Beschreiben Sie das Problem und die entsprechenden Bedingungen möglichst genau.

Fügen Sie Ihrer Anfrage unbedingt eine Datei mit dem vollständigen Speicherabbild des Betriebssystem Microsoft Windows bei. Diese Datei wird folgendermaßen erstellt:

1. Klicken Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz** und wählen Sie im folgenden Fenster den Punkt **Eigenschaften**.
2. Wählen Sie im folgenden Fenster **Systemeigenschaften** die Registerkarte **Erweitert** und klicken Sie im Abschnitt **Starten und Wiederherstellen** auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im Fenster **Starten und Wiederherstellen** im Abschnitt **Debuginformationen speichern** aus der Dropdown-Liste den Wert **Vollständiges Speicherabbild**.

   Die Datei mit dem Speicherabbild wird standardmäßig unter dem Namen *memory.dmp* im Systemverzeichnis gespeichert. Sie können einen anderen Ordner zum Speichern des Dumps festlegen. Ändern Sie dazu im entsprechenden Feld den Ordnernamen.

4. Wiederholen Sie den Vorgang, bei dem das mit der Arbeit von Kaspersky Internet Security verbundene Problem aufgetreten ist.
5. Vergewissern Sie sich, dass die Datei mit dem vollständigen Speicherabbild erfolgreich gespeichert wurde.

ANHANG A. ZUSÄTZLICHE INFORMATIONEN

Dieser Anhang enthält Informationen über die Formate von zu untersuchenden Dateien und über zulässige Masken, die bei der Konfiguration von Kaspersky Internet Security verwendet werden können.

A.1. Liste der Objekte, die nach Erweiterung untersucht werden

Wenn Sie für die Untersuchungsobjekte von Datei-Anti-Virus die Option **Programme und Dokumente (nach Erweiterung) untersuchen** gewählt haben, dann werden die Dateien mit den unten aufgezählten Erweiterungen ausführlich auf Viren analysiert. Die gleichen Dateien werden auch von Mail-Anti-Virus untersucht, wenn die Filterung von Objekten aktiviert ist, die an E-Mails angehängt sind:

com – ausführbare Programmdatei.

exe – ausführbare Datei, selbstextrahierendes Archiv.

sys – Systemtreiber.

prg – Text der Programme dBase, Clipper oder Microsoft Visual FoxPro, Programm des Pakets WAVmaker.

bin – Binärdatei.

bat – Datei einer Paketaufgabe.

cmd – Befehlsdatei für Microsoft Windows NT (entspricht einer bat-Datei für DOS), OS/2.

dpl – komprimierte Bibliothek für Borland Delphi.

dll – Dynamic Link Library (Dynamische Verbindungsbibliothek).

scr – Bildschirmschonerdatei für Microsoft Windows.

cpl – Systemsteuerungsmodul (control panel) in Microsoft Windows.

ocx – Microsoft OLE-Objekt (Object Linking and Embedding).

tsp – Programm, das im Timesharing-Modus arbeitet.

drv – Treiber für ein bestimmtes Gerät.

vxd – Treiber für ein virtuelles Microsoft-Windows-Gerät.

pif – Datei mit Informationen zum Programm.

lnk – Linkdatei in Microsoft Windows.

reg – Registrierungsdatei für Schlüssel der Microsoft-Windows-Systemregistrierung.

ini – Initialisierungsdatei.

cla – Java-Klasse.

vbs – Visual-Basic-Skript.

vbe – BIOS-Video-Erweiterung.

js, jse – JavaScript-Quelltext.

htm – Hypertext-Dokument.

htt – Hypertext-Entwicklung von Microsoft Windows.

hta – Hypertext-Programm für Microsoft Internet Explorer.

asp – Active-Server-Pages-Skript.

chm – kompilierte HTML-Datei.

pht – HTML-Datei mit eingebettetem PHP-Skript.

php – Skript, das in eine HTML-Datei eingebettet wird.

wsh – Microsoft Windows Script Host-Datei.

wsf – Microsoft-Windows-Skript.

the – Bildschirmschonerdatei für den Arbeitsplatz von Microsoft Windows 95

hlp – Hilfedatei des Formats Win Help.

eml – E-Mail-Nachricht für Microsoft Outlook Express.

nws – neue E-Mail-Nachricht für Microsoft Outlook Express.

msg – E-Mail-Nachricht für Microsoft Mail.

plg – E-Mail-Nachricht

mbx – Erweiterung für eine gespeicherte Nachricht in Microsoft Office Outlook.

doc – Microsoft Office Word-Dokument.

dot – Microsoft Office Word-Dokumentvorlage.

fpm – Datenbankprogramm, Startdatei für Microsoft Visual FoxPro.

rtf – Dokument im Rich-Text-Format.

shs – Fragment für Shell Scrap Object Handler.

dwg – Datenbank für AutoCAD-Skizzen.

msi – Microsoft Windows Installer-Paket.

otm – VBA-Projekt für Microsoft Office Outlook.

pdf – Adobe Acrobat-Dokument.

swf – Shockwave Flash-Paketobjekt.

jpg, jpeg – Grafikdatei zum Speichern von komprimierten Bildern.

emf – Datei des Formats Enhanced Metafile. Folgegeneration einer Metadatei des Betriebssystems Microsoft Windows. EMF-Dateien werden von 16-Bit-Microsoft Windows nicht unterstützt.

ico – Symboldatei für ein Objekt.

ov? – ausführbare Datei für MS DOS.

*xl** – Dokumente und Dateien für Microsoft Office Excel, z.B.: *xla* – Erweiterung für Microsoft Office Excel, *xlc* – Diagramm, *xlt* – Dokumentvorlage usw.

*pp** – Dokumente und Dateien für Microsoft Office PowerPoint, z.B.: *pps* – Dia für Microsoft Office PowerPoint, *ppt* – Präsentation usw.

*md** – Dokumente und Dateien für Microsoft Office Access, z.B.: *mda* – Arbeitsgruppe für Microsoft Office Access, mdb – Datenbank usw.

Beachten Sie, dass das tatsächliche Format einer Datei von dem Format abweichen kann, das in der Dateierweiterung angegeben ist.

A.2. Zulässige Ausschlussmasken für Dateien

Hier werden Beispiele für zulässige Masken genannt, die Sie beim Erstellen der Liste auszuschließender Dateien verwenden können:

1. Masken ohne Dateipfad:
   - ***.exe** – alle Dateien mit der Endung *exe*
   - ***.ex?** – alle Dateien mit der Endung *ex?*, wobei anstelle von ? ein beliebiges Zeichen stehen kann.
   - **test** – alle Dateien mit dem Namen *test*
2. Masken mit absolutem Dateipfad:
   - **C:\dir*.*** oder **C:\dir*** oder **C:\dir** – alle Dateien im Ordner *C:\dir*
   - **C:\dir*.exe** – alle Dateien mit der Endung *exe* im Ordner *C:\dir*
   - **C:\dir*.ex?** – alle Dateien mit der Endung *ex?* im Ordner *C:\dir*, wobei anstelle von ? ein beliebiges Zeichen stehen kann.
   - **C:\dir\test** – nur die Datei *C:\dir\test*

Um zu verhindern, dass die Dateien in allen untergeordneten Ordnern des gewählten Ordners untersucht werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen **Unterordner einschließen**.

3. Masken mit relativem Dateipfad:

   - **dir*.*** oder **dir*** oder **dir** – alle Dateien in allen Ordnern von *dir*
   - **dir\test** – alle Dateien *test* in den Ordnern von *dir*
   - **dir*.exe** – alle Dateien mit der Endung *exe* in allen Ordnern von *dir*
   - **dir*.ex?** – alle Dateien mit der Endung *ex?* in allen Ordnern von *dir\,* wobei anstelle von ? ein beliebiges Zeichen stehen kann.

   Um zu verhindern, dass die Dateien in allen untergeordneten Ordnern des gewählten Ordners untersucht werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen **Unterordner einschließen**.

Hinweis:

Die Verwendung der Ausnahmemasken ***.*** oder * ist nur unter Angabe der Klassifikation der auszuschließenden Bedrohung entsprechend der Viren-Enzyklopädie zulässig. In diesem Fall wird die Bedrohung nicht in allen Objekten gefunden werden. Die Verwendung dieser Masken ohne Angabe einer Klassifikation entspricht dem Deaktivieren des Echtzeitschutzes.

Außerdem wird davor gewarnt, als Ausnahme ein virtuelles Laufwerk zu wählen, das auf der Basis eines Ordners des Dateisystems mit dem Befehl *subst* erstellt wurde. Dies wäre sinnlos, da das Programm das virtuelle Laufwerk bei der Untersuchung als Ordner betrachten und folglich untersuchen würde.

A.3. Zulässige Ausschlussmasken nach der Klassifikation der Viren-Enzyklopädie

Wenn eine Bedrohung mit einem bestimmten Status nach der Klassifikation der Viren-Enzyklopädie als Ausnahme hinzugefügt wird, können Sie angeben:

- den vollständigen Namen der Bedrohung, wie er in der Viren-Enzyklopädie auf der Seite www.viruslist.de genannt wird (beispielsweise **not-a-virus:RiskWare.RemoteAdmin.RA.311** oder **Flooder.Win32.Fuxx**).
- den Namen der Bedrohung als Maske, beispielsweise:
    - **not-a-virus*** – legale, aber potentiell gefährliche Programme sowie Scherzprogramme von der Untersuchung ausschließen.
    - ***Riskware.*** – alle potentiell gefährlichen Programme des Typs Riskware von der Untersuchung ausschließen.
    - ***RemoteAdmin.*** – alle Programmversionen zur entfernten Verwaltung von der Untersuchung ausschließen.

ANHANG B. KASPERSKY LAB

Das Unternehmen

Kaspersky Lab ist ein weltweit führendes Unternehmen in den Bereichen Viren-, Spam- und Hacker-Schutz. Unser hoch spezialisiertes Viren-Labor reagiert stets schneller als alle anderen auf neue Bedrohungen, so dass unsere innovativen Programme seit vielen Jahren Heimanwender und Unternehmen jeder Größe zuverlässig schützen.

Bereits 1997 wurde Kaspersky Lab von dem russischen Virenexperten Eugene Kaspersky in Moskau gegründet und hat heute unter anderem Niederlassungen in Deutschland, Frankreich, Großbritannien, Polen, Japan, USA und China.

Einzigartige Erfahrung

Weltweit beschäftigt Kaspersky Lab über 550 hochspezialisierte Mitarbeiter, darunter Mitglieder der Computer Anti-Virus Researchers Organisation (CARO) und des Virus Bulletin Technical Advisory Board. Im Laufe vieler Jahre Forschung und Kampf gegen Computerviren haben wir Wissen und Fähigkeiten erworben, die heute unser wertvollstes Kapital darstellen.

Dank unserer weit reichenden Erfahrung sind wir in der Lage, Entwicklungstrends bei Malware vorherzusehen. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab, so dass wir anderen immer einen Schritt voraus sind und unseren Kunden stets den besten Schutz bieten können.

Kaspersky Anti-Virus

Nach vielen Jahren innovativer Entwicklungen zählt Kaspersky Lab heute zu den führenden Herstellern von Sicherheits-Software. Der hohe Standard unserer Produkte wird durch zahlreiche Auszeichnungen internationaler Forschungseinrichtungen, unabhängiger Testlabors und renommierter Fachpublikationen bestätigt.

Die Programm-Module unseres bekanntesten Programms, Kaspersky Anti-Virus, gewährleisten einen zuverlässigen Schutz für Workstations, Datei- und Web-Server, Mail-Gateways, Firewalls, Pocket-PCs und Smartphones.

Als erstes Unternehmen entwickelte Kaspersky Lab bedeutende Technologien, die heute selbst bei zahlreichen Antiviren-Programmen anderer Hersteller – wie G-Data, Aladdin und F-Secure – als Programm-Kern einen unverzichtbaren Bestandteil bilden. So vertrauen bereits über 200 Millionen Anwender unseren Innovationen, wie dem heuristischen Analysator zur Entdeckung noch unbekannter Viren, den Micro-Updates für die Antiviren-Datenbanken und dem ersten umfassenden Virenschutz für Unix/Linux-Systeme.

Komplexe Technologien für Ihre Sicherheit

Moderne Viren und Schadprogramme sind komplexe Bedrohungen, so dass die bisher üblichen Schutzpakete für PCs und Netzwerke häufig nicht mehr ausreichen.

Aus diesem Grund entwickelte Kaspersky Lab mit Kaspersky Anti-Hacker eine Personal Firewall und mit Kaspersky Anti-Spam einen besonders effektiven Spam-Filter. Mit den Produkten von Kaspersky Lab können Sie Ihren Computer und Ihr Netzwerk optimal vor allen modernen virtuellen Gefahren schützen.

Service

Kaspersky Lab bietet seinen Kunden eine ganze Palette zusätzlicher Dienstleistungen, die einen maximalen Schutz garantieren: Die Antiviren-Datenbanken werden stündlich aktualisiert, die Anti-Spam-Dateien 12 bis 24 Mal pro Tag. Zudem steht allen Anwendern ein rund-um-die-Uhr-Support zur Verfügung: Telefonisch oder per E-Mail – in deutscher, englischer, russischer und französischer Sprache.

B.1. Weitere Produkte und Services von Kaspersky Lab

Kaspersky Lab News Agent

Das Programm News Agent dient der schnellen Zustellung der Nachrichten von Kaspersky Lab, der Benachrichtigung über das "Virus-Wetter" und über neu erschienene Nachrichten. Das Programm liest in vorgegebenen Zeitabständen von den Kaspersky-Lab-Newsservern eine Liste der verfügbaren Nachrichtenkanäle und der darin enthaltenen Informationen.

News Agent verfügt außerdem über folgende Funktionen:

- Visualisierung des Zustands des "Viren-Wetters" im Infobereich der Taskleiste.
- Abonnieren und Abbestellen der Nachrichtenkanäle von Kaspersky Lab.
- Download von Nachrichten für jeden abonnierten Kanal in festgelegten Zeitabständen. Außerdem erfolgt eine Benachrichtigung über ungelesene Nachrichten.
- Anzeige von Nachrichten der abonnierten Kanäle.
- Anzeige einer Liste der Kanäle und ihrer Status.
- Öffnen der Webseite mit dem vollständigen Nachrichtentext im Browser.

News Agent funktioniert unter dem Betriebssystem Microsoft Windows. Er kann als separates Produkt benutzt werden oder zu unterschiedlichen integrierten Lösungen von Kaspersky Lab gehören.

Kaspersky OnLine Scanner

Dieses Programm ist ein kostenloser Dienst, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antivirenuntersuchung des Computers im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Webbrowser ausgeführt. Dadurch kann der Benutzer auf schnelle Weise herausfinden, ob sein Computer von einer Infektion durch schädliche Programme bedroht ist. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Antiviren-Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

Kaspersky® OnLine Scanner Pro

Dieses Programm stellt einen Abonnementsdienst dar, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antivirenuntersuchung des Computers und die Desinfektion infizierter Dateien im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Webbrowser ausgeführt. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Antiviren-Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 dient dem Schutz eines Personalcomputers vor schädlichen Programmen. Dabei werden traditionelle Virenschutzmethoden auf optimale Weise mit neuen proaktiven Technologien vereinigt.

Das Programm erlaubt eine komplexe Antivirenuntersuchung, die folgende Optionen umfasst:

- Antivirenuntersuchung des Mail-Datenstroms auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm, sowie Untersuchung und Desinfektion von Mail-Datenbanken.

- Antivirenuntersuchung des Internet-Datenstroms, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- Antivirenuntersuchung beliebiger einzelner Dateien, Ordner und Laufwerke. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystem Microsoft Windows gestartet werden, vorhanden.

Der Proaktive Schutz umfasst:

- **Kontrolle über Veränderungen im Dateisystem**. Das Programm erlaubt es, eine Liste der Anwendungen anzulegen, deren Komponentenbestand kontrolliert werden soll. Dadurch lässt sich die Verletzung der Integrität von Anwendungen durch Schadprogramme verhindern.
- **Überwachung von Prozessen im Arbeitsspeicher**. Kaspersky Anti-Virus 6.0 warnt den Benutzer rechtzeitig, wenn gefährliche, verdächtige oder versteckte Prozesse auftreten oder wenn normale Prozesse auf unerlaubte Weise verändert werden.
- **Überwachung von Veränderungen in der Registrierung des Betriebssystems** durch die Kontrolle des Zustands der Systemregistrierung.
- **Sperren gefährlicher Makros** des Typs Visual Basic for Applications in Microsoft Office Dokumenten.
- **Systemwiederherstellung** nach schädlicher Einwirkung von Spyware: Die Wiederherstellung wird durch die Speicherung aller Veränderungen in der Registrierung und im Dateisystem des Computers und durch das vom Benutzer initiierte Rückgängigmachen der Veränderungen ermöglicht.

Kaspersky® Security für PDA

Kaspersky® Security für PDA gewährleistet zuverlässigen Virenschutz für Daten auf Handheld-PCs unter Palm OS oder Microsoft Windows CE sowie für Daten, die von einem gewöhnlichen PC oder Erweiterungsspeichern, von CD-ROM oder aus Datenbanken übernommen werden. Das Programm umfasst eine optimale Auswahl an Virenschutz-Komponenten:

- einen Virenscanner, der eine Überprüfung der Daten (sowohl im Speicher des PDA selbst, als auch auf beliebigen Speicher-Erweiterungskarten) auf Anforderung des Anwenders ausführt;
- den Antivirus-Monitor, der während der Synchronisation über HotSync™ und während des Datenaustausches mit anderen PDA Virenprogramme blockiert.

Weiterhin schützt das Programm die auf dem PDA gespeicherten Informationen vor unberechtigtem Zugriff durch Verschlüsselung des Zugriffs auf das Gerät

selbst wie auch auf die im Speicher des PDA und auf Speicherkarten enthaltenen Daten.

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile bietet den Antivirenschutz für mobile Geräte, die mit den Betriebssystemen Symbian OS und Microsoft Windows Mobile arbeiten. Das Programm erlaubt es, eine komplexe Antivirenuntersuchung vorzunehmen, die folgende Optionen umfasst:

- **Scan auf Befehl** des Arbeitsspeichers, der Speicherkarten, einzelner Ordner oder einer konkreten Datei des mobilen Geräts. Wenn ein infiziertes Objekt gefunden wird, wird es in den Quarantäneordner verschoben oder gelöscht.
- **Echtzeit-Untersuchung**: alle eingehenden oder veränderten Objekte und alle Dateien, auf die versucht wird zuzugreifen, werden automatisch untersucht.
- **Untersuchung nach Zeitplan** von Informationen, die im Arbeitsspeicher des mobilen Geräts gespeichert sind.
- **Schutz vor sms- und mms-Spam**.

Kaspersky Anti-Virus® Business Optimal

Dieses Programmpaket ist die ultimative Lösung zum Schutz vor Computerviren für Unternehmen kleiner und mittlerer Größe.

Kaspersky Anti-Virus® Business Optimal bietet Rundumschutz[3] vor Viren für:

- Computerarbeitsplätze unter Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation, Linux.
- Dateiserver unter Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD und Linux; Dateispeicher unter Samba.
- Mailsysteme vom Typ Microsoft Exchange 2000/2003, Lotus Notes/Domino, postfix, exim, sendmail und qmail.
- Internet-Gateways: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition, Microsoft ISA Server 2004 Standard Edition.

Kaspersky Anti-Virus® Business Optimal beinhaltet außerdem das zentrale Installations- und Administrationssystem Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

---

[3] Je nach Lieferumfang

Kaspersky® Corporate Suite

Kaspersky® Corporate Suite ist eine integrierte Softwarelösung zum Datenschutz für Ihr gesamtes Firmennetzwerk ohne Einschränkungen hinsichtlich Größe und Struktur. Die enthaltenen Programmkomponenten schützen jeden Punkt ihres firmeninternen Netzes. Sie sind kompatibel mit den meisten heute verbreiteten Betriebssystemen und Anwendungen, über ein zentrales Steuerungssystem miteinander verbunden und werden über eine gemeinsame Benutzeroberfläche bedient. Mit diesem System erhalten Sie einen Virenschutz, der sich vollständig an die Systemanforderungen Ihres internen Netzes anpassen lässt.

Kaspersky® Corporate Suite bietet Rundumschutz[4] vor Viren für:

- Computerarbeitsplätze unter Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation und Linux.
- Dateiserver unter Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, Linux; Dateispeicher unter Samba.
- Mailsysteme vom Typ Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, sendmail, postfix, exim und qmail.
- Internet-Gateways: CheckPoint Firewall –1; Microsoft ISA Server 2000 Enterprise Edition; Microsoft ISA Server 2004 Enterprise Edition.
- Handheld-PCs, die unter Symbian OS, Microsoft Windows CE und Palm OS arbeiten, sowie Smartphones, die unter Microsoft Windows Mobile 2003 for Smartphone und Microsoft Smartphone 2002 arbeiten.

Kaspersky® Corporate Suite beinhaltet außerdem das zentrale Installations- und Administrationssystem Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam ist die erste in Russland entwickelte Software zum Schutz vor unerwünschten Mailings (Spam) für Unternehmen kleinerer und mittlerer Größe. Das Programm vereint moderne Verfahren der Sprachanalyse für Informationen in Textform, sämtliche modernen Verfahren zum Filtern von E-Mails (einschließlich RBL-Listen und formeller Prüfung von Nachrichten) sowie eine einmalige Auswahl an Dienstprogrammen, durch die der Nutzer in die Lage versetzt wird, bis zu 95 % der unerwünschten Nachrichten zu identifizieren und zu eliminieren.

[4] Je nach Lieferumfang

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am „Eingang“ des firmeninternen Netzwerks installiert, sämtliche eingehenden Mitteilungen auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

Die tägliche Aktualisierung der Filterdatenbank mit Mustertexten aus unserem Sprachlabor garantiert eine hohe Effizienz dieses Produkts. Die Datenbank-Updates erscheinen alle 20 Minuten.

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux / Unix dient der Antivirenbearbeitung von E-Mails, die mit SMTP-Protokoll weitergeleitet werden. Die Anwendung umfasst eine Reihe von zusätzlichen Filterinstrumenten für den Mailverkehr (Filterung nach Namen und MIME-Typen von Attachments) sowie eine Reihe von Mitteln, die es erlauben, die Belastung des Mailsystems zu verringern und Hackerangriffe abzuwehren. Dazu zählen die Begrenzung der maximalen Mailgröße, der Anzahl von Adressaten usw. Die Unterstützung der Technologie DNS Black List schützt vor dem Empfang von Mails, die von Servern stammen, die auf diesen Listen stehen und als Verbreitungsquellen für Spam gelten.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security® for Microsoft Exchange bietet die Antivirenuntersuchung der eingehenden, ausgehenden und auf dem Server gespeicherten E-Mail-Nachrichten einschließlich der Nachrichten in gemeinsamen Ordnern. Außerdem führt er die Filterung unerwünschter Korrespondenz aus, wobei intelligente Technologien zur Spam-Erkennung in Verbindung mit Technologien der Firma Microsoft verwendet werden. Die Anwendung untersucht alle mit dem SMTP-Protokoll auf dem Exchange-Server eingehenden Nachrichten auf das Vorhandensein von Viren, wobei Antivirentechnologien von Kaspersky Lab verwendet werden, und auf Spam-Merkmale, wozu die Filterung nach formalen Kennzeichen (E-Mail-Adresse, IP-Adresse, Größe der Mail, Kopfzeile) dient. Außerdem analysiert er den Inhalt des Briefs und seiner Anhänge mit Hilfe von intelligenten Technologien, die unikale grafische Signaturen zum Erkennen von Spam in grafischer Form umfassen. Der Untersuchung werden sowohl der Nachrichtenkörper als auch angehängte Dateien unterzogen.

Kaspersky® Mail Gateway

Kaspersky® Mail Gateway ist eine universelle Lösung für den komplexen Schutz der Benutzer von Mailsystemen. Die Anwendung wird zwischen dem Unternehmensnetzwerk und dem Internet installiert und führt die Untersuchung aller Elemente einer E-Mail auf das Vorhandensein von Viren und anderen schädlichen Programmen (Spyware, Adware usw.) durch. Außerdem erfolgt die zentralisierte Filterung des E-Mail-Nachrichtenstroms auf Spam-Merkmale. Die Anwendung enthält eine Reihe von Zusatzwerkzeugen zur Filterung des Mail-Datenstroms – nach Namen und MIME-Typen der angehängten Dateien, sowie

eine Reihe von Mitteln, die es erlauben, die Belastung des Mailsystems zu senken und Hackerangriffe zu verhindern.

Kaspersky Anti-Virus® for Proxy Server

Kaspersky Anti-Virus® for Proxy Server ist eine Antivirenlösung für den Schutz des Web-Datenverkehrs, der mit dem HTTP-Protokoll über einen Proxyserver geleitet wird. Die Anwendung führt im Echtzeitmodus die Antivirenuntersuchung des Internet-Datenverkehrs durch, schützt vor dem Eindringen schädlicher Programme während des Surfens im Web und scannt Dateien, die aus dem Internet heruntergeladen werden.

Kaspersky Anti-Virus® for MIMESweeper for SMTP

Kaspersky Anti-Virus® for MIMESweeper for SMTP bietet die Hochgeschwindigkeits-Antivirenuntersuchung des SMTP-Datenverkehrs auf Servern, die Clearswift MIMESweeper verwenden.

Das Programm besitzt die Form eines PlugIns für die Anwendung MIMESweeper for SMTP der Firma Clearswift und führt im Echtzeitmodus die Antivirenuntersuchung und –bearbeitung des ein- und ausgehenden Mailverkehrs durch.

B.2. Kontaktinformationen

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gern umfassend per Telefon oder E-Mail beraten.

Weitere Information erhalten Sie bei:

Kaspersky Labs GmbH

Steinheilstraße 13

85053 Ingolstadt

Technischer Support	Tel.: +49 (0) 841 98 18 90 Fax: +49 (0) 841 98 18 918 E-Mail: support@kaspersky.de
Allgemeine Informationen	WWW: http://www.kaspersky.de/ http://www.viruslist.de/
Feedback zu unseren Benutzerhand-büchern	docfeedback@kaspersky.com (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

ANHANG C. ENDBENUTZER-LIZENZVERTRAG

Endbenutzer-Lizenzvertrag für die erworbene KASPERSKY LAB SOFTWARE

WICHTIG - bitte sorgfältig lesen: Lesen Sie die in diesem KASPERSKY LAB Endbenutzer-Lizenzvertrag ("EULA") beschriebenen Rechte und Einschränkungen sorgfältig durch. Sie werden gebeten, die Bestimmungen des EULAs zu prüfen und ihnen zuzustimmen oder diese abzulehnen.

Indem Sie das Sicherheitsetikett auf der CD-Box aufreißen oder wenn Sie die SOFTWARE installieren, erklären Sie sich mit den Bestimmungen des EULAs einverstanden. Falls Sie mit den Bestimmungen des EULAs NICHT einverstanden sind, geben Sie die erworbene Software bitte innerhalb von 14 Tagen an die Einkaufsstelle zurück. Nach Eingabe des Aktivierungscodes ist eine Rückgabe der Software ausgeschlossen.

Jede Bezugnahme auf "Software" schließt den Aktivierungscode oder die Schlüsseldatei ein, den Sie von Kaspersky Lab als Teil der Software erhalten.

Dieser EULA ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Besitzer eines Exemplars der SOFTWARE (entweder als natürlicher oder als juristischer Person) und KASPERSKY LAB. KASPERSKY LAB wird sich das exklusive Urheberrecht auf die Computersoftware (auf die Software und die Antiviren-Datenbanken) vorbehalten. Indem Sie die SOFTWARE installieren, erklären Sie sich damit einverstanden, durch die Bestimmungen dieses EULAs gebunden zu sein. Falls Sie den Bestimmungen dieses EULAs nicht zustimmen, sind Sie nicht berechtigt, die SOFTWARE zu installieren und zu verwenden.

Die SOFTWARE ist sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum geschützt. Die SOFTWARE wird lizenziert, nicht verkauft.

1. LIZENZEINRÄUMUNG. Durch diesen EULA werden Ihnen folgende Rechte eingeräumt:

> • Sie sind berechtigt, eine Kopie der SOFTWARE auf einem einzigen Computer zu installieren und zu verwenden. Eine Mehrplatzlizenz der SOFTWARE, dürfen Sie auf so vielen Computern installieren, wie Sie Lizenzen erworben haben.
>
> • Sie sind berechtigt, die installierte SOFTWARE innerhalb der erworbenen Lizenzdauer zu benutzen.

2. EINSCHRÄNKUNGEN

> • Einschränkungen im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, die SOFTWARE zurückzuentwickeln (Reverse Engineering), zu dekompilieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet. Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.

• Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.

• Supportleistungen. Nach Kauf und Aktivierung der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die Lizenzdauer. Supportleistungen verstehen sich wie folgt:

– stündliche Updates der Antiviren-Datenbank

– kostenloses Updates der Software

– kostenlose technische Unterstützung sowohl per e-Mail als auch per Telefon mit KASPERSKY LAB

3. KÜNDIGUNG. Unbeschadet sonstiger Rechte ist KASPERSKY LAB berechtigt, diesen EULA zu kündigen, sofern Sie gegen die Bestimmungen dieses EULAs verstoßen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien der SOFTWARE und alle ihre Komponenten zu vernichten.

4. URHEBERRECHT. Eigentum und Urheberrecht auf die SOFTWARE, die gedruckten Begleitmaterialien und jede Kopie der SOFTWARE liegen bei KASPERSKY LAB.

5. GEWÄHRLEISTUNG. KASPERSKY LAB gewährleistet, dass:

• die SOFTWARE den Spezifikationen im wesentlichen entspricht.

• im Falle einer physikalischen Lieferung der Originaldatenträger frei von Material- und Herstellungsfehlern ist.

• das Programm korrekt auf den Datenträger aufgezeichnet ist, die Dokumentation sämtliche Informationen enthält, die KASPERSKY LAB für die Benutzung der Software für erforderlich hält.

• die SOFTWARE binnen 90 Tagen ab der ersten Installation oder dem ersten Download, falls richtig behandelt, der in der beiliegenden Dokumentation bestimmten Funktionalität entspricht und laut derer voll funktionsfähig ist.

Gewährleistungspflichtige Mängel werden von KASPERSKY LAB oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der Gewährleistungsfrist, dem Ermessen von Kaspersky Lab nach, durch Ersatz, Reparatur, Umtausch oder Rückzahlung beseitigt, falls eine Mangelrüge rechtzeitig an Kaspersky Lab oder dessen Lieferanten gerichtet wurde. KASPERSKY LAB oder dessen Lieferanten übernehmen keine Gewährleistung für Mängel, die auf andere als für die Software vorgesehenen Einsatzbedingungen, unsachgemäße Behandlung oder dergleichen zurückzuführen sind.

ALLE ANDERE GEWÄHRLEISTUNGEN UND BEDINGUNGEN, SEIEN SIE AUSDRÜCKLICH ODER KONKLUDENT, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF, (FALLS ZUTREFFEND) JEDE KONKLUDENTE GEWÄHRLEISTUNG IM HINBLICK AUF HANDELSÜBLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, FAHRLÄSSIGKEIT ODER MANGELNDE FACHMÄNNISCHE BEMÜHUNGEN WERDEN VON KASPERSKY LAB ODER DESSEN LIEFERANTEN ABGELEHNT. ES BESTEHT EBENFALLS KEINE GEWÄHRLEISTUNG ODER BEDINGUNG VON RECHTSANSPRÜCHEN IN BEZUG AUF RECHTSINHABERSCHAFT, UNGESTÖRTES NUTZUNGVERGNÜGEN ODER NICHTVERLETZUNG VON RECHTEN DRITTER. DAS GESAMTE RISIKO, DAS BEI DER BENUTZUNG ODER LEISTUNG DER SOFTWARE ENTSTEHT, LIEGT BEI IHNEN.

6. AUSSCHLUSS DER HAFTUNG FÜR ALLE SCHÄDEN. SOWEIT GESETZLICH ZUGELASSEN, SIND KASPERSKY LAB ODER DESSEN LIEFERANTEN IN KEINEM FALL HAFTBAR FÜR IRGENDWELCHE FOLGE-, ZUFÄLLIGEN, DIREKTEN, INDIREKTEN, SPEZIELLEN, STRAFRECHTLICHEN ODER ANDEREN SCHÄDEN WELCHER ART AUCH IMMER (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AN PERSONEN ODER SACHEN, SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG, VERLUST VON GESCHÄFTLICHEN INFORMATIONEN, FÜR DEN VERLUST VON PRIVATSPHÄRE, DIE UNMÖGLICHKEIT, EINE PFLICHT ZU ERFÜLLEN (EINSCHLIESSLICH GEMÄSS TREU UND GUTEN GLAUBENS ODER VERNÜNFTIGER ANGEMESSENER SORGFALT) ZU ERFÜLLEN, FÜR FAHRLÄSSIGKEIT ODER ANDERE VERMÖGENSSCHÄDEN), DIE AUS DER VERWENDUNG DER SOFTWARE ODER DER TATSACHE, DASS SIE NICHT VERWENDET WERDEN KANN, RESULTIEREN ODER DAMIT IN ZUSAMMENHANG STEHEN, SELBST WENN KASPERSKY LAB ODER DESSEN LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WORDEN IST. DIESER HAFTUNGSAUSSCHLUSS FÜR SCHÄDEN GILT AUCH DANN, WENN ABHILFEMASSNAHMEN IHREN WESENTLICHEN ZWECK VERFEHLEN.

7. ANWENDBARES RECHT. Dieser Vertrag unterliegt der Gesetzgebung des Landes, indem das Produkt erworben wurde.